

How to configure VPN function on TP-LINK Routers

| | | |
|----|---|----|
| 1. | VPN Overview..... | 2 |
| 2. | How to configure LAN-to-LAN IPsec VPN on TP-LINK Router..... | 3 |
| 3. | How to configure GreenBow IPsec VPN Client with a TP-LINK VPN Router..... | 13 |
| 4. | How to configure Shrew Soft VPN IPsec Client with TP-LINK Router..... | 23 |
| 5. | How to configure LAN-to-LAN L2TP/PPTP VPN on TP-LINK Router | 34 |
| 6. | How to configure a PPTP Server on TP-LINK Router | 41 |
| 7. | How to configure a L2TP Server on TP-LINK Router..... | 53 |

1. VPN Overview

VPN (Virtual Private Network) is a private network established via the public network, generally via the Internet. However, the private network is a logical network without any physical network lines, so it is called Virtual Private Network.

With the wide application of the Internet, more and more data are needed to be shared through the Internet. Connecting the local network to the Internet directly, though can allow the data exchange, will cause the private data to be exposed to all the users on the Internet. The VPN (Virtual Private Network) technology is developed and used to establish the private network through the public network, which can guarantee a secured data exchange.

VPN adopts the tunneling technology to establish a private connection between two endpoints. It is a connection secured by encrypting the data and using point-to-point authentication. As the packets are encapsulated and de-encapsulated in the Router, the tunneling topology implemented by encapsulating packets is transparent to users.

The tunneling protocols supported by TP-LINK Routers are as below:

| Product Model | Tunneling Protocol |
|---------------|--------------------|
| TL-ER6120 | IPsec、PPTP、L2TP |
| TL-ER6020 | IPsec、PPTP、L2TP |
| TL-ER604W | IPsec、PPTP、L2TP |
| TL-R600VPN | IPsec、PPTP |

2. How to configure LAN-to-LAN IPsec VPN on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W, TL-R600VPN



To setup an IPsec VPN tunnel on TP-LINK routers you need to perform the following steps:

- A. Connecting the devices together
- B. Verify the settings needed for IPsec VPN on router
- C. Configuring IPsec VPN settings on TL-ER6120 (Router A)
- D. Configuring IPsec VPN settings on TL-R600VPN (Router B)
- E. Checking IPsec SA

NOTE: We use TL-ER6120 and TL-R600VPN in this example, the way to configure IPsec VPN on TL-ER6020/TL-ER604W is the same as that on TL-ER6120.

A. Connecting the devices together

Before setup a VPN tunnel, you need to ensure that the two routers are connected to the Internet. After ensuring that there is an active Internet connection on each router, you need to verify the VPN settings of the two routers, please follow the instruction below.

B. Verify the settings needed for IPsec VPN on router

To verify the settings needed on the two routers, please login the router's management webpage.

Router A's Status page:

TP-LINK

TL-ER6120

Network

- Status
- System Mode
- WAN
- LAN
- DMZ
- MAC Address
- Switch

User Group

Advanced

Firewall

VPN

Services

Maintenance

Logout

System Status

Device Info

Firmware Version:

1.0.0 Build 20111114 Rel.52682

Hardware Version:

TL-ER6120 v1.0

System Time

System Time:

2012-02-08 10:11:16 Wednesday

Running Time:

14 Hour, 34 Min, 53 Sec

WAN

WAN1

Link Up

Primary Connection:

PPPoE/Russian PPPoE

Status:

Connected

Online Time:

6 Sec

IP Address:

218.18.0.233

Subnet Mask:

255.255.255.255

MAC Address:

90-F6-52-49-A0-67

Secondary Connection:

Status:

IP Address:

Subnet Mask:

WAN2

Link Down

Primary Connection:

Dynamic IP

Status:

Connecting...

IP Address:

0.0.0.0

Subnet Mask:

0.0.0.0

Gateway:

0.0.0.0

MAC Address:

90-F6-52-49-A0-68

Secondary Connection:

Status:

IP Address:

Subnet Mask:

This will be Router B's Remote Gateway IP

This is Router A's Local Subnet

LAN/DMZ

Router B's Status page:

TP-LINK

Status

Firmware Version: 1.0.0 Build 120118 Rel.41877n
Hardware Version: R600VPN v1 00000000

LAN

MAC Address: 90-F6-52-26-1C-44
IP Address: 192.168.10.1
Subnet Mask: 255.255.255.0

WAN

MAC Address: 90-F6-52-26-1C-45
IP Address: 218.18.1.208
Subnet Mask: 255.255.255.255
Default Gateway: 218.18.1.208
DNS Server: 202.96.134.33, 202.96.128.86
Online Time: 0 day(s) 00:04:49

Disconnect

C. Configuring IPsec VPN settings on TL-ER6120 (Router A)

Step 1 : On the management webpage, click on VPN then IKE Proposal.

Under IKE Proposal, enter Proposal Name whatever you like, select Authentication, Encryption and DH Group, we use MD5,3DES, DH2 in this example.

TP-LINK

TL-ER6120

IKE Policy **IKE Proposal**

IKE Proposal

Proposal Name: test1
Authentication: MD5
Encryption: 3DES
DH Group: DH2

List of IKE Proposal

| No. | Name | Auth | Encr | DH | Action |
|-------------|------|------|------|----|--------|
| No entries. | | | | | |

Select All Delete Search

Step 2 : Click on Add.

Step 3 : Click on IKE Policy, enter Policy Name whatever you like, select Exchange Mode, in this example we use Main, select IP Address as ID Type.

Step 4 : Under IKE Proposal 1, we use test1 in this example. Enter Pre-shared Key and SA Lifetime you want, DPD is disabled.

Step 5 : Click on Add.

Step 6 : Click on IPsec on the left menu, then IPsec Proposal. Select Security Protocol, ESP Authentication and ESP Encryption you want to enable on VPN tunnel. Here we use ESP, MD5 and 3DES for example.

Step 7 : Click on Add.

Step 8 : Click on IPsec Policy, enter Policy Name whatever you like, the Mode should be LAN-to-LAN. Enter Local Subnet and Remote Subnet.

Step 9 : Select WAN you use and type in Remote Gateway. In this example, the Remote Gateway is Router B's WAN IP address, 218.18.1.208.

Step 10 : Look for Policy Mode and select IKE.

Step 11 : Under IKE Policy, we select test1 which is used.

Step 12 : Under IPsec Proposal, we use ipsec1 in this example.

Step 13 : Look for PFS, we set NONE here, under SA Lifetime, enter "28800" or the period you want.

Step 14 : Look for Status then select Activate

The screenshot shows the IPsec Policy configuration interface. On the left is a sidebar with links: L2TP/PPTP, Services, Maintenance, and Logout. The main area contains configuration fields for Local Subnet (192.168.0.0/24), Remote Subnet (192.168.10.0/24), WAN, Remote Gateway (192.168.0.1), Policy Mode (IKE selected), IKE Policy (test1), IPsec Proposal 1 (ipsec1), IPsec Proposal 2 (----), IPsec Proposal 3 (----), IPsec Proposal 4 (----), PFS (NONE), SA Lifetime (28800), and Status (Activate selected). A table below lists the IPsec Policy with one entry: No. 1, Name ipsec, Local Subnet 192.168.0.0/24, Remote Subnet 192.168.10.0/24, Policy Mode IKE. Annotations include: 'Select IKE' pointing to the Policy Mode dropdown; 'test1 and ipsec1 are used' pointing to the IKE Policy and IPsec Proposal 1 dropdowns; 'Enter "28800"' pointing to the SA Lifetime field; and 'Select Activate' pointing to the Status dropdown.

Copyright © 2011 TP-LINK TECHNOLOGIES CO., LTD. All Rights Reserved.

Step 15 : Click on Add.

The screenshot shows the IPsec Policy configuration page with the 'IPsec Policy' tab selected. The 'General' section has 'IPsec' set to 'Disable'. The 'IPsec Policy' section has 'Policy Name' (ipsec), 'Mode' (LAN-to-LAN), and 'Local Subnet' (192.168.0.0/24). On the right, there are buttons: Save, Add, Clear, and Help. An annotation 'Click on Add' points to the 'Add' button.

Step 16 : Select Enable then click on Save.

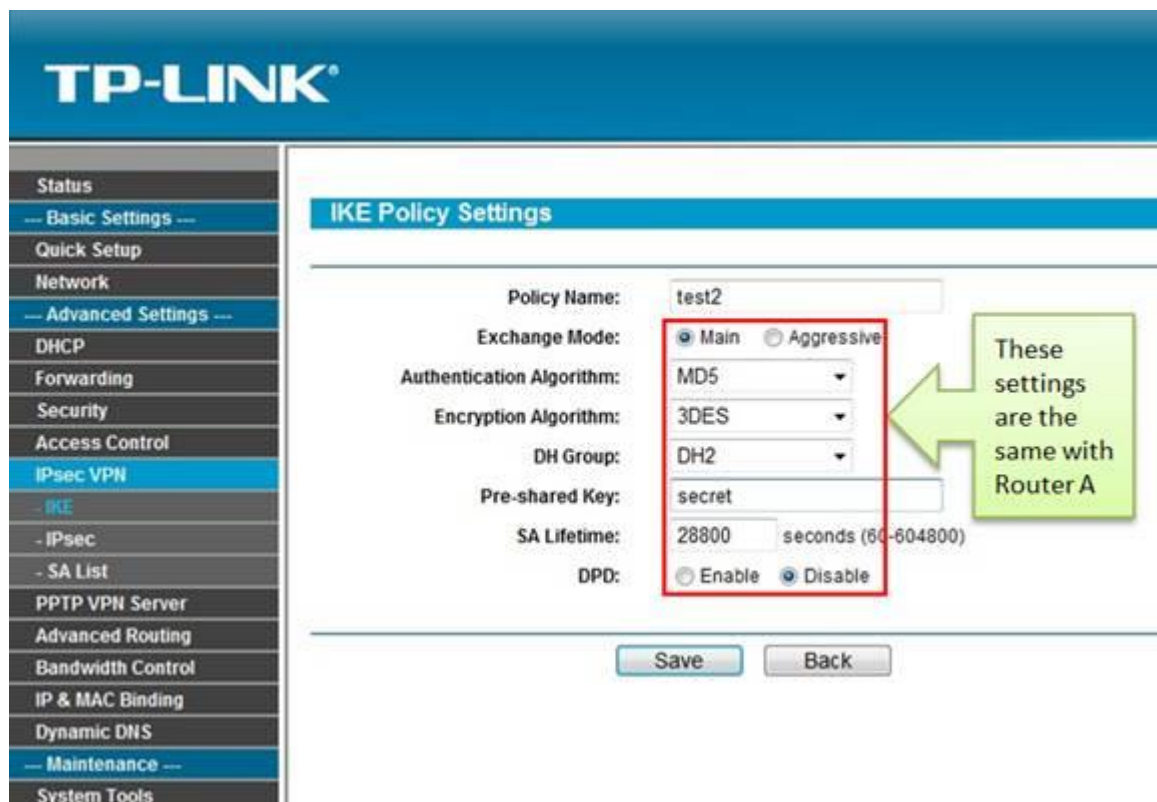
The screenshot shows the IPsec Policy configuration page with the 'IPsec Policy' tab selected. The 'General' section has 'IPsec' set to 'Enable'. The 'IPsec Policy' section has 'Policy Name' (ipsec), 'Mode' (LAN-to-LAN), and 'Local Subnet' (192.168.0.0/24). On the right, there are buttons: Add, Clear, and Help. An annotation 'Select Enable' points to the 'Enable' radio button, and another annotation 'Click on Save' points to the 'Save' button.

D. Configuring IPsec VPN settings on TL-R600VPN (Router B)

Step 1 : Go to IPsec VPN -> IKE, click on Add New



Step 2 : Enter Policy Name whatever you like, here we use test2. Exchange Mode, select Main.



Step 3 : Authentication Algorithm and Encryption Algorithm are the same with Router A, we use MD5 and 3DES in this example.

Step 4 : DH Group, select DH2, the same with Router A.

Step 5 : Enter Pre-share Key and SA Lifetime, make sure that they are the same with Router A.

Step 6 : Click on Save.

Step 7 : Click on IPsec on left side, click on Add New.



Step 8 : Enter Policy Name, we use ipsec2 in this example.

Step 9 : Enter Local Subnet and Remote Subnet, and then enter Remote Gateway, it's Router A's WAN IP address, 218.18.0.233.



Step 10 : Look for Exchange mode, please select IKE, and Security Protocol, we use ESP here.

Step 11 : Authentication Algorithm and Encryption Algorithm are the same with Router A, we use MD5 and 3DES in this example.

Step 12 : IKE Security Policy, we use test2 in this example.

Step 13 : Look for PFS, we set NONE here, under Lifetime, enter "28800" or the period you want.

Step 14 : Look for Status then select Enable.

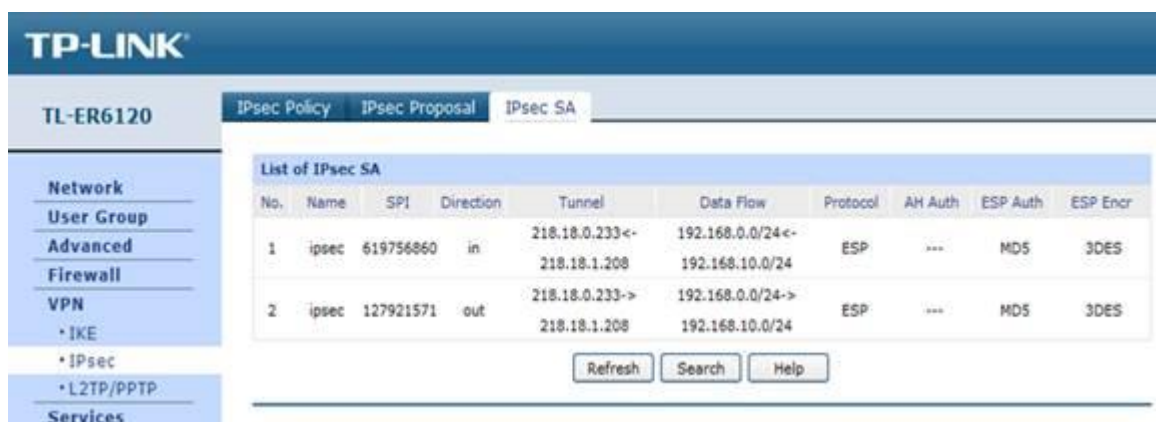
Step 15 : Click on Save.

Step 16 : Enable IPsec and then click on Save.



E. Checking IPsec SA

Router A:



Router B:

Status

--- Basic Settings ---

Quick Setup

Network

--- Advanced Settings ---

DHCP

Forwarding

Security

Access Control

IPsec VPN

- IKE

- IPsec

- SA List

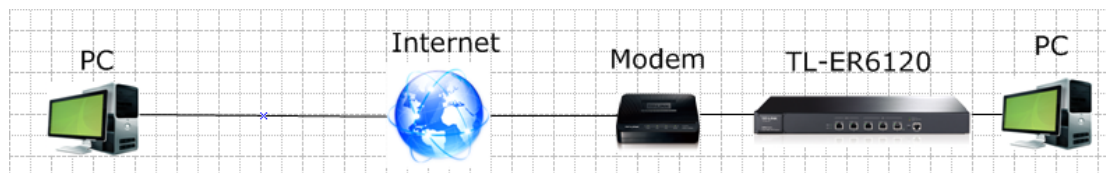
List of Security Association

| ID | Name | SPID | Tunnel Initiator | Tunnel Receiver | Security Protocol | AH Auth | ESP Auth | ESP Encr |
|----|--------|-----------|------------------|-----------------|-------------------|---------|----------|----------|
| 1 | ipsec2 | 619756860 | 218.18.1.208 | 218.18.0.233 | ESP | -- | MD5 | 3DES |
| 2 | ipsec2 | 127921571 | 218.18.0.233 | 218.18.1.208 | ESP | -- | MD5 | 3DES |

Refresh

3. How to configure GreenBow IPsec VPN Client with a TP-LINK VPN Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



GreenBow IPsec VPN Client is an IPsec VPN client software developed by TheGreenBow company. It can be downloaded from download page for TL-ER6120 (<http://www.tp-link.com/en/support/download/?model=TL-ER6120&version=V1>) or official website of TheGreenBow (http://www.thegreenbow.com/vpn/vpn-client.html?utm_expid=333874-5.xSdTaggCQhu28X37j2BKrw.1&utm_referrer=http%3A%2F%2Fwww.thegreenbow.com%2Fservices.html).

To setup an IPsec VPN tunnel between the GreenBow IPsec VPN Client and the TP-LINK VPN Router you need to perform the following steps:

- A. Make sure PCs of two sides can access to Internet**
- B. Configuring the TP-LINK VPN Router**
- C. Configuring the GreenBow VPN Client**

A. Make sure PCs of two sides can access to Internet

Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring the TP-LINK VPN Router

Step 1:

Access the router's management webpage, verify the settings needed on the router.

| Device Info | |
|-------------------|--------------------------------|
| Firmware Version: | 1.0.2 Build 20120719 Rel.42888 |
| Hardware Version: | TL-ER6120 v1.0 |

| System Time | |
|---------------|-------------------------------|
| System Time: | 2012-09-05 16:07:49 Wednesday |
| Running Time: | 5 Day, 4 Hour, 46 Min, 5 Sec |



| WAN | |
|-----------------------|---------------------|
| WAN1 | Link Up |
| Primary Connection: | PPPoE/Russian PPPoE |
| Status: | Connected |
| Online Time: | 5 Min, 49 Sec |
| IP Address: | 183.14.247.247 |
| Subnet Mask: | 255.255.255.255 |
| MAC Address: | 90-F6-52-BD-EE-FB |
| Secondary Connection: | --- |
| Status: | --- |
| IP Address: | --- |
| Subnet Mask: | --- |

| LAN/DMZ | | | | |
|-----------|-------------|---------------|-------------|-------------------|
| Interface | IP Address | Subnet Mask | DHCP Server | MAC Address |
| LAN | 192.168.0.1 | 255.255.255.0 | Enabled | 90-F6-52-BD-EE-FA |

Step 2:

On the management webpage, click on VPN then IKE Proposal. Under IKE Proposal, enter Proposal Name whatever you like, select Authentication, Encryption and DH Group, we use MD5, 3DES, DH2 in this example.

| IKE Proposal | |
|-----------------|------|
| Proposal Name: | 1 |
| Authentication: | MD5 |
| Encryption: | 3DES |
| DH Group: | DH2 |

| List of IKE Proposal | | | | | | |
|--------------------------|-----|------|------|------|-----|---|
| | No. | Name | Auth | Encr | DH | Action |
| <input type="checkbox"/> | 1 | 1 | MD5 | 3DES | DH2 |   |

Step 3:

Click on IKE Policy, enter Policy Name whatever you like, select Exchange Mode, in this example we use Main, select FQDN as ID Type and enter Local ID and Remote ID whatever you like, here we enter "1234" for Local ID and "4321" for Remote ID.

IKE Policy

| | | |
|-----------------|--|--|
| Policy Name: | <input type="text" value="123"/> | |
| Exchange Mode: | <input checked="" type="radio"/> Main <input type="radio"/> Aggressive | <input type="button" value="Save"/> <input type="button" value="Clear"/> <input type="button" value="Help"/> |
| Local ID Type: | <input type="radio"/> IP Address <input checked="" type="radio"/> FQDN | |
| Local ID: | <input type="text" value="1234"/> | |
| Remote ID Type: | <input type="radio"/> IP Address <input checked="" type="radio"/> FQDN | |
| Remote ID: | <input type="text" value="4321"/> | |
| IKE Proposal 1: | <input type="text" value="1"/> | |
| IKE Proposal 2: | <input type="text" value="----"/> | |
| IKE Proposal 3: | <input type="text" value="----"/> | |
| IKE Proposal 4: | <input type="text" value="----"/> | |
| Pre-shared Key: | <input type="text" value="123456"/> | |
| SA Lifetime: | <input type="text" value="28800"/> Sec (1-6) | |
| DPD: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| DPD Interval: | <input type="text" value="0"/> Sec (1-300) | |

Here we enter
123456
 as Pre-shared Key

NOTE: No matter on Main mode or Aggressive mode, once the client PC is behind a NAT device, we have to select FQDN as ID Type and the NAT device must support VPN passthrough, otherwise the VPN tunnel can't be established.

Step 4:

Under IKE Proposal 1, we select 1 in this example. Enter Pre-shared Key and SA Lifetime you want, DPD is disabled.

Step 5:

Click on IPsec on the left menu, then IPsec Proposal. Select Security Protocol, ESP Authentication and ESP Encryption you want to enable on VPN tunnel. Here we use ESP, MD5 and 3DES for example.

IPsec Proposal

Proposal Name:

Security Protocol:

ESP Authentication:

ESP Encryption:

List of IPsec Proposal

| | No. | Name | Protocol | AH Auth | ESP Auth | ESP Encr | Action |
|--------------------------|-----|------|----------|---------|----------|----------|---|
| <input type="checkbox"/> | 1 | 123 | ESP | --- | MD5 | 3DES |   |

Step 6:

Click on IPsec Policy, enter Policy Name whatever you like, the Mode should be Client-to-LAN. Enter Local Subnet and select WAN port.

General

IPsec: ☒ Enable ☐ Disable

IPsec Policy

Policy Name:

Mode:

Local Subnet: /

Remote Subnet: /

WAN:

Remote Host:

Policy Mode: ☒ IKE ☐ Manual

IKE Policy:

IPsec Proposal 1:

IPsec Proposal 2:

IPsec Proposal 3:

IPsec Proposal 4:

PFS:

SA Lifetime: Sec (120-604800)

Status: ☒ Activate ☐ Inactivate

Select
Client-
to-LAN

Step 7:

Look for Policy Mode and select IKE. Under IKE Policy, we select 123 which is used. Under IPsec Proposal, we use 123 in this example.

Step 8:

Look for PFS, we set NONE here, under SA Lifetime, enter "28800" or the period you want.
Look for Status then select Activate.

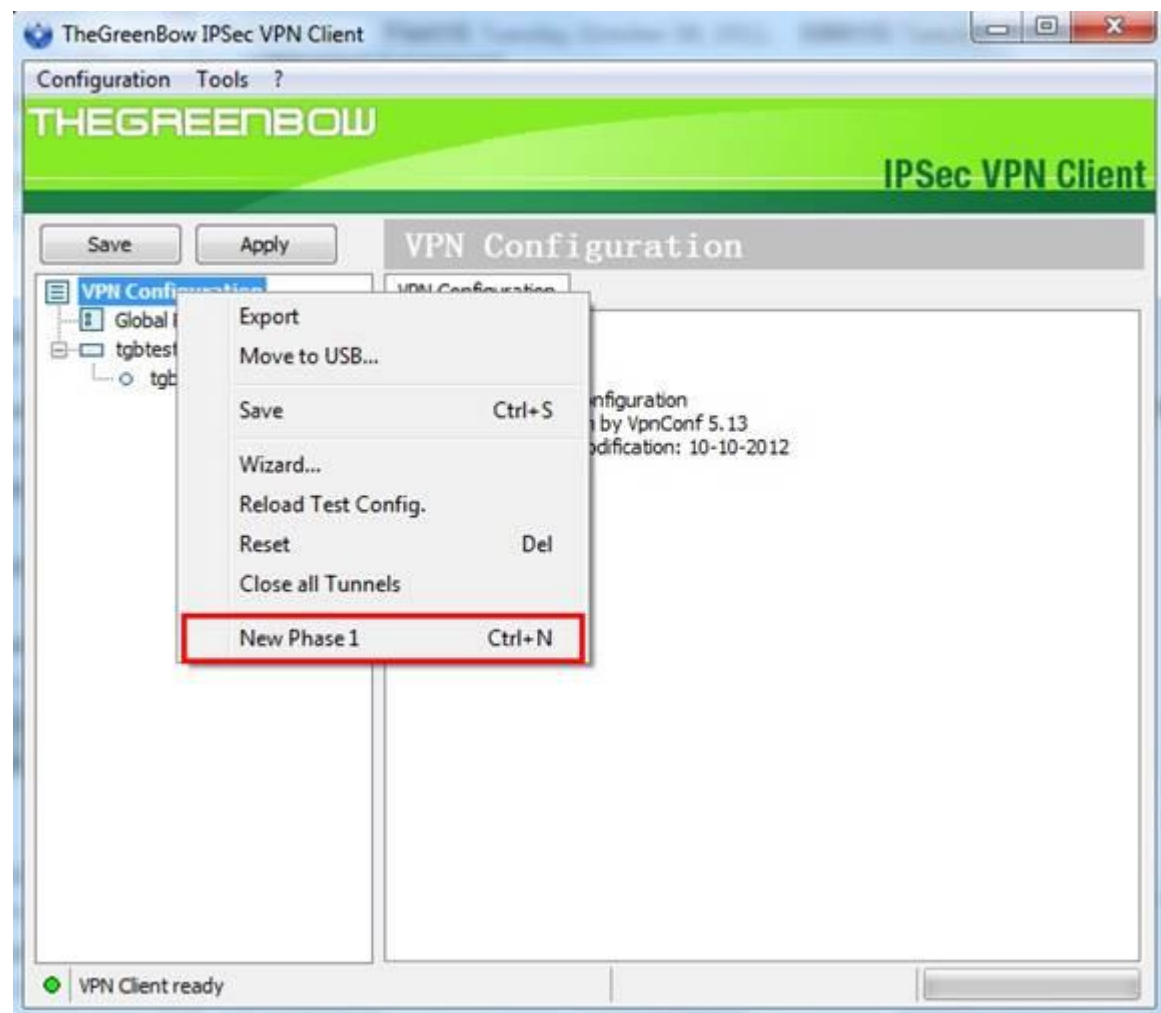
Step 9:

Enable IPsec and then click on Save.

C. Configuring the GreenBow VPN Client

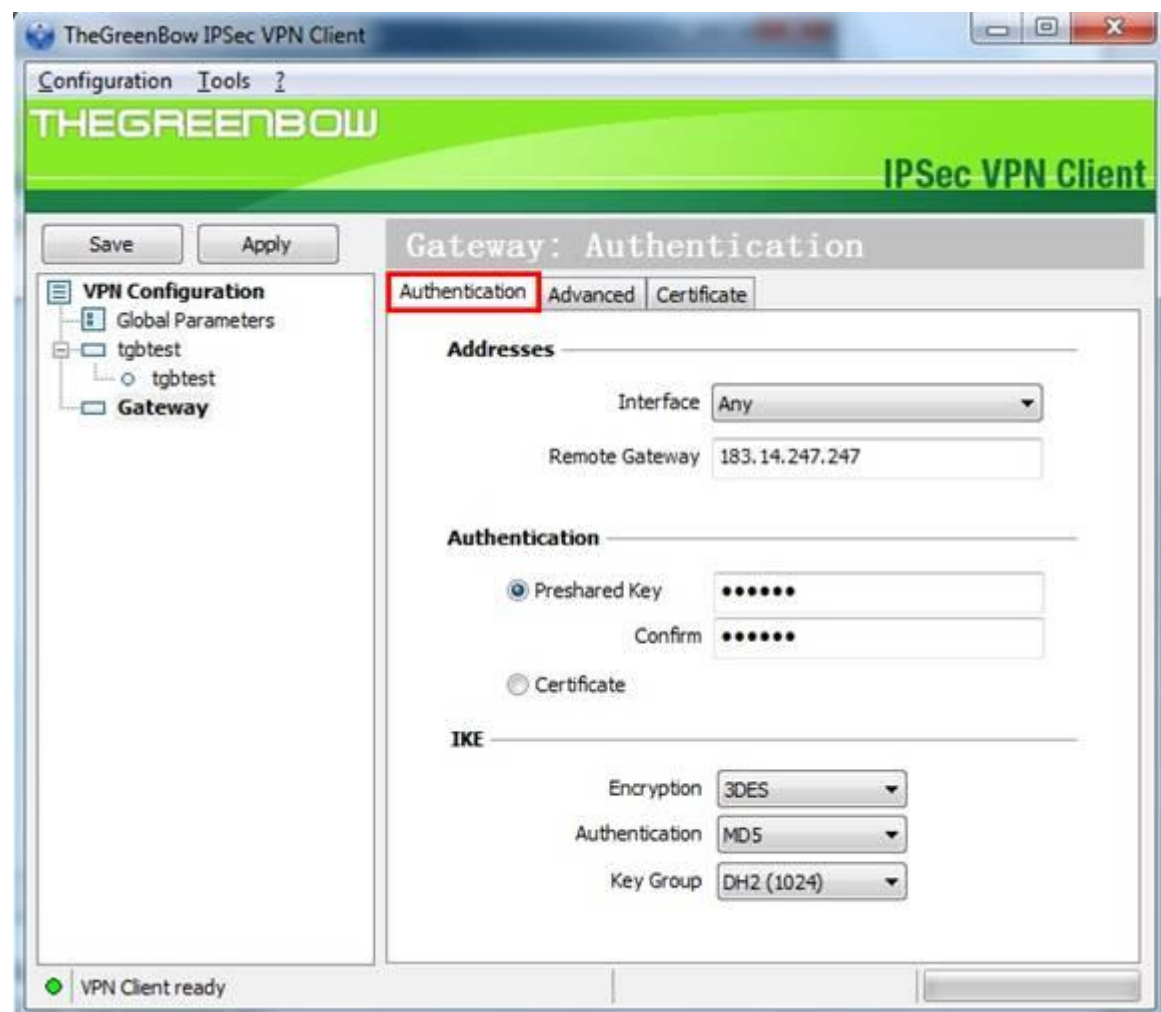
Step 1:

Right click on VPN Configuration and click on New Phase 1.



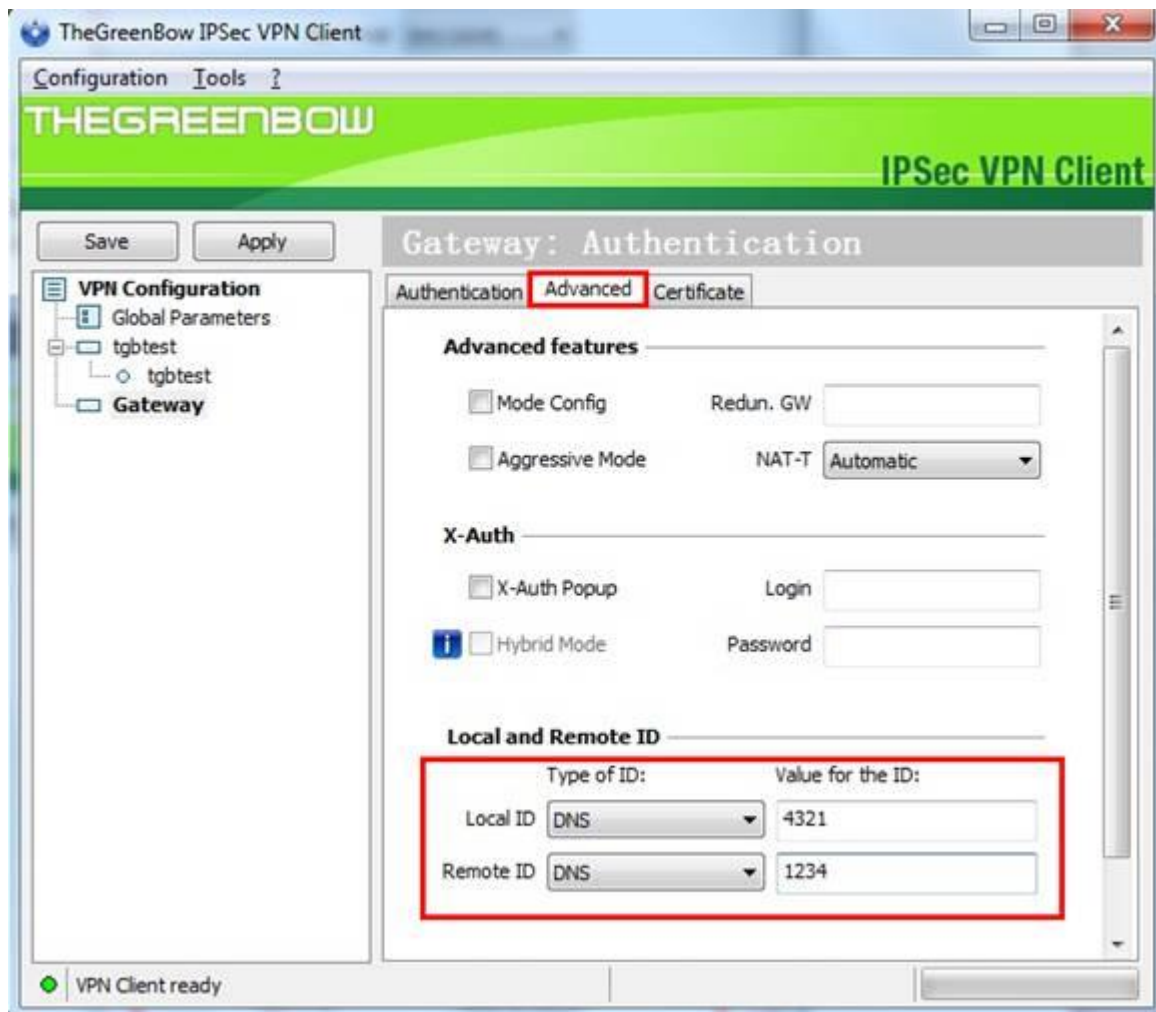
Step 2:

Under Remote Gateway, enter the router's WAN IP address, the Pre-shared Key should be the same with router's, it is "123456".on IKE section, the Encryption, Authentication and Key Group are the same with router's, we use 3DES, MD5and DH2 here.



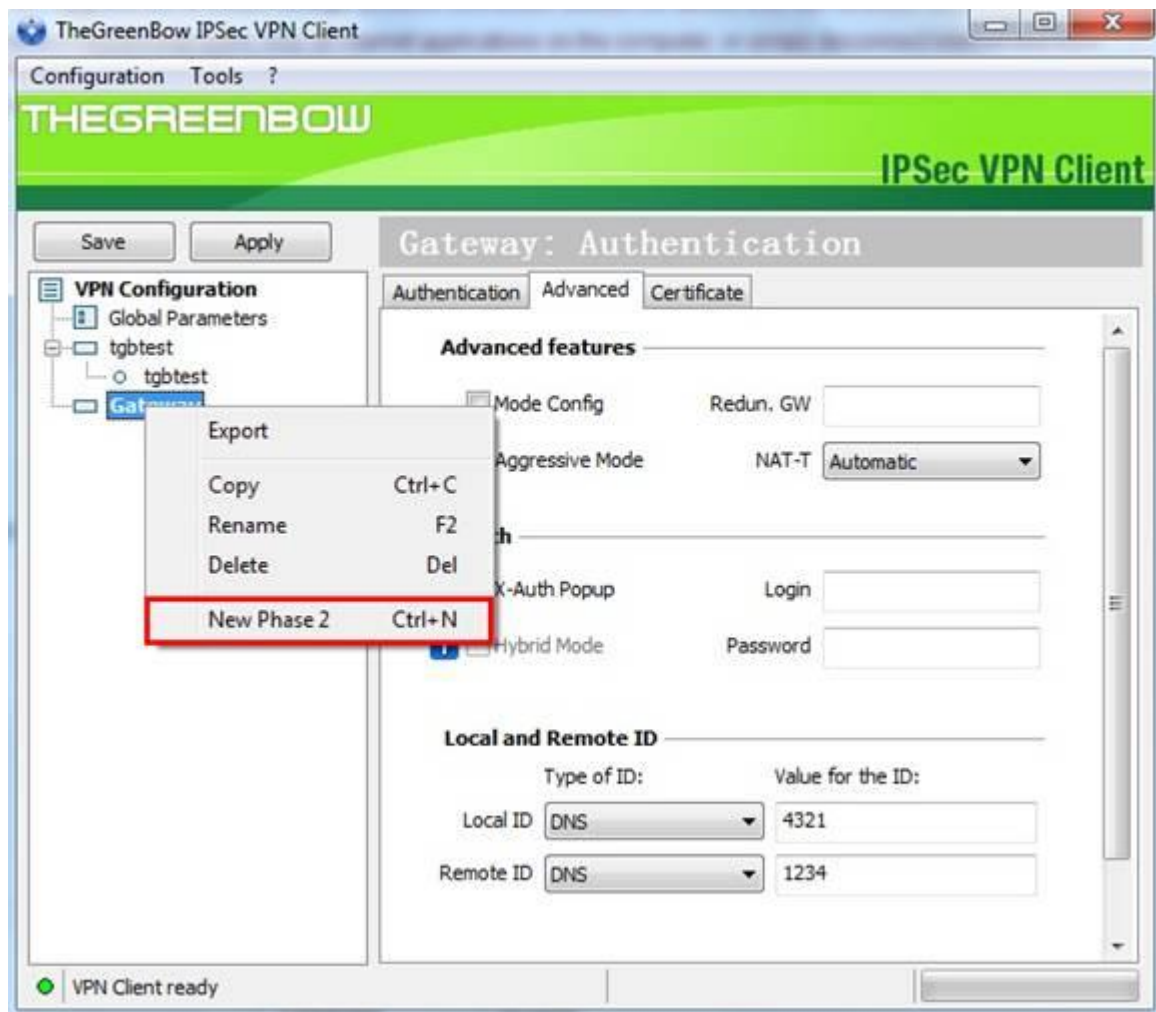
Step 3:

Go to Advanced tab, select DNS as Type of ID, and then enter "4321" for Local ID and "1234" for Remote ID.



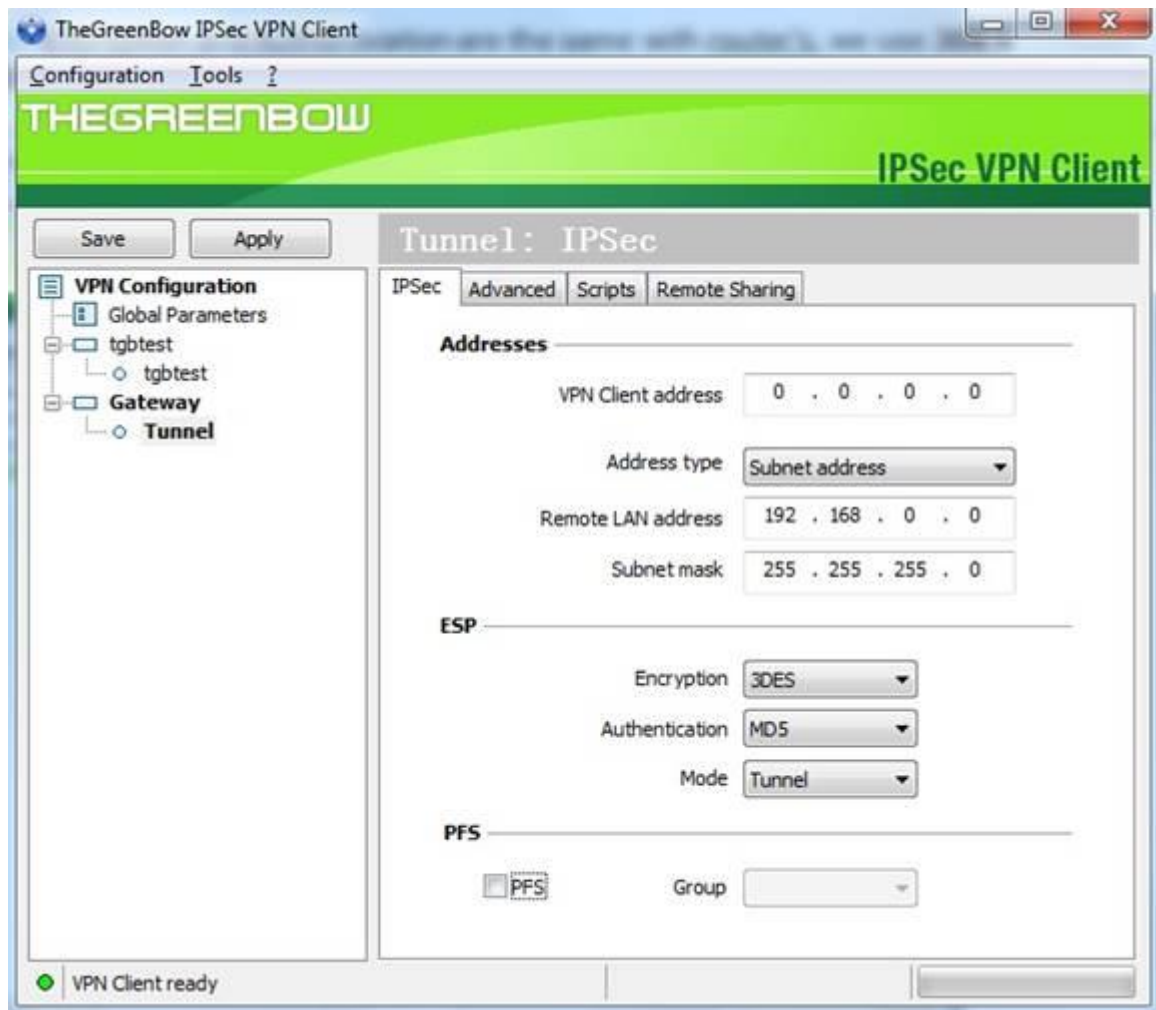
Step 4:

Right click on Phase 1, add a new phrase 2.



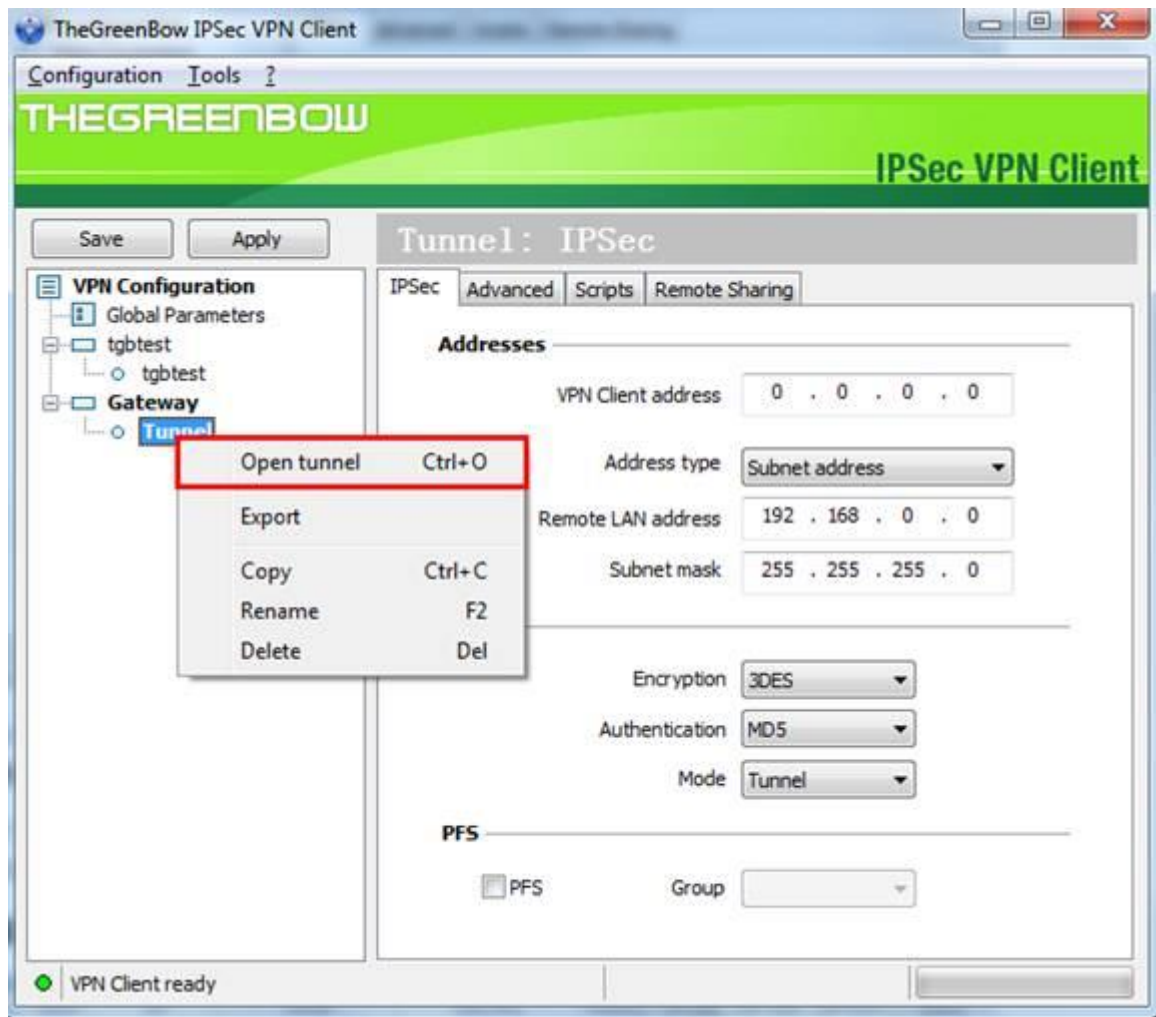
Step 5:

Enter remote LAN address and Subnet mask, in the example, the IP address is 192.168.0.0, Subnet mask is 255.255.255.0. Encryption and Authentication are the same with routers; we use 3DES and MD5 here. The Mode should be Tunnel.



Step 6:

Click Save and Apply and then right click on Phrase 2(Tunnel), click on Open Tunnel.



Step 7:

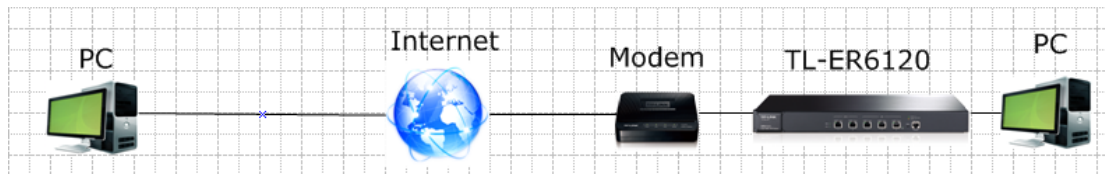
If the client connect to the VPN Server successfully, you can see IPsec SA on the list.

| IPsec Policy IPsec Proposal IPsec SA | | | | | | | | | | |
|--|------|-----------------------------|------------------------------------|---------------------------------------|----------|---------|----------|----------|-----------|--|
| List of IPsec SA | | | | | | | | | | |
| No. | Name | SPI | Tunnel | Data Flow | Protocol | AH Auth | ESP Auth | ESP Encr | Status | |
| 1 | 123 | 2646071062<-> 1641697897 | 183.14.247.247<-> 183.37.236.61 | 192.168.0.0/24<-> 192.168.1.100/32 | ESP | --- | MD5 | 3DES | Connected | |

Refresh Search Help

4. How to configure Shrew Soft VPN IPsec Client with TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



Shrew Soft VPN IPsec Client is an VPN Client software developed by Shrew Soft Inc. It can be downloaded from official website of Shrew Soft (<https://www.shrew.net/download/vpn>).

To set up an IPsec VPN tunnel, you need to perform the following steps:

- A. Make sure PCs of two sides can access to Internet**
- B. Configuring IPsec VPN settings on TL-ER6120**
- C. Configuring the Shrew VPN Client**

A. Make sure PCs of two sides can access to Internet

Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring IPsec VPN settings on TL-ER6120

Step 1: Access the router's management webpage; verify the settings needed on the router.

TL-ER6120

System Status

Device Info

Firmware Version: 1.0.3 Build 20121022 Rel.54185
Hardware Version: TL-ER6120 v1.0

System Time

System Time: 2012-10-26 17:42:31 Friday
Running Time: 37 Min, 28 Sec

WAN

| WAN1 | Link Up | WAN2 | Link Down |
|--------------------------------|---------|--------------------------------|-----------|
| Primary Connection: Dynamic IP | | Primary Connection: Dynamic IP | |
| Status: Connected | | Status: Connecting... | |
| IP Address: 10.10.10.156 | | Address: 0.0.0.0 | |
| Subnet Mask: 255.255.255.0 | | Subnet Mask: 0.0.0.0 | |
| Gateway: 10.10.10.1 | | Gateway: 0.0.0.0 | |
| MAC Address: 90-F6-52-BD-EE-FB | | MAC Address: 90-F6-52-BD-EE-FC | |
| Secondary Connection: --- | | Secondary Connection: --- | |
| Status: --- | | Status: --- | |
| IP Address: --- | | IP Address: --- | |
| Subnet Mask: --- | | Subnet Mask: --- | |

LAN/DMZ

| Interface | IP Address | Subnet Mask | DHCP Server | MAC Address |
|-----------|-------------|---------------|-------------|-------------------|
| LAN | 192.168.1.1 | 255.255.255.0 | Enabled | 90-F6-52-BD-EE-FA |

Annotations:

- This LAN Subnet Address is for Shrew's Remote Network Resource (points to 192.168.1.1)
- This is for Shrew's Host Name or IP Address (points to 10.10.10.156)

Step 2: On the management webpage, click on VPN then IKE Proposal. Under IKE Proposal, enter Proposal Name whatever you like, select Authentication, Encryption and DH Group, we use MD5, 3DES, DH2 in this example. Click on Add.

TL-ER6120

IKE Policy **IKE Proposal**

IKE Proposal

Proposal Name: test

Authentication: MD5

Encryption: 3DES

DH Group: DH2

Buttons: Add, Clear, Help

List of IKE Proposal

| No. | Name | Auth | Encr | DH | Action |
|-------------|------|------|------|----|--------|
| No entries. | | | | | |

Buttons: Select All, Delete, Search

Step 3: Click on IKE Policy, enter Policy Name whatever you like, we select Aggressive for Exchange Mode, select FQDN as ID Type and enter Local ID whatever you like, here we enter "123" for Local ID and "321" for Remote ID.

TL-ER6120

IKE Policy

IKE Proposal

Network

User Group

Advanced

Firewall

VPN

• IKE

• IPsec

• L2TP/PPTP

Services

Maintenance

Logout

IKE Policy

Policy Name:

ike

Exchange Mode:

☐ Main
 ☒ Aggressive

Local ID Type:

☐ IP Address
 ☒ FQDN

Local ID:

123

Remote ID Type:

☐ IP Address
 ☒ FQDN

Remote ID:

321

IKE Proposal 1:

test

IKE Proposal 2:

IKE Proposal 3:

IKE Proposal 4:

Pre-shared Key:

123456789

SA Lifetime:

28800

Sec (60-604800)

DPD:

☐ Enable
 ☒ Disable

DPD Interval:

15

Sec (1-300)

Add

Clear

Help

List of IKE Policy

| No. | Name | Mode | Proposal 1 | Proposal 2 | Proposal 3 | Proposal 4 | Action |
|-------------|------|------|------------|------------|------------|------------|--------|
| No entries. | | | | | | | |

Select All

Delete

Search

NOTE: No matter on Main mode or Aggressive mode, once the client PC is behind a NAT device, we have to select FQDN as ID Type and the NAT device must support VPN passthrough, otherwise the VPN tunnel can't be established.

Step 4: Under IKE Proposal 1, we select test in this example. Enter Pre-shared Key and SA Lifetime you want, DPD is disabled. Click on Add.

Step 5: Click on IPsec on the left menu, then IPsec Proposal. Select Security Protocol, ESP Authentication and ESP Encryption you want to enable on VPN tunnel. Here we use ESP, MD5 and 3DES for example. Click on Add.

TL-ER6120

Network

User Group

Advanced

Firewall

VPN

• IKE

• **IPsec**

• L2TP/PPTP

Services

Maintenance

Logout

IPsec Policy

IPsec Proposal

IPsec SA

IPsec Proposal

Proposal Name:

test

Security Protocol:

ESP

ESP Authentication:

MD5

ESP Encryption:

3DES

Add

Clear

Help

List of IPsec Proposal

| No. | Name | Protocol | AH Auth | ESP Auth | ESP Encr. | Action |
|-------------|------|----------|---------|----------|-----------|--------|
| No entries. | | | | | | |

Select All

Delete

Search

Step 6: Click on IPsec Policy, enter Policy Name whatever you like, the Mode should be Client-to-LAN. Enter Local Subnet and select WAN port.

TP-LINK

TL-ER6120

IPsec Policy

IPsec Proposal

IPsec SA

Network

User Group

Advanced

Firewall

VPN

• IKE

• **IPsec**

• L2TP/PPTP

Services

Maintenance

Logout

General

IPsec:

☒ Enable
 ☐ Disable

Save

IPsec Policy

Policy Name:

ipsec

Mode:

Client-to-LAN

Local Subnet:

192.168.1.0 / 24

Remote Subnet:

0.0.0.0 / 0

WAN:

WAN1

Remote Host:

0.0.0.0

Policy Mode:

☒ IKE
 ☐ Manual

IKE Policy:

ike

IPsec Proposal 1:

test

IPsec Proposal 2:

IPsec Proposal 3:

IPsec Proposal 4:

PFS:

NONE

SA Lifetime:

28800

Sec (120-604800)

Status:

☒ Activate
 ☐ Inactivate

Add

Clear

Help

List of IPsec Policy

| No. | Name | Mode | Local Subnet | Remote Subnet | Policy Mode | Status | Action |
|-------------|------|------|--------------|---------------|-------------|--------|--------|
| No entries. | | | | | | | |

Select All

Activate

Inactivate

Delete

Search

Copyright © 2011

Step 7: Look for Policy Mode and select IKE. Under IKE Policy, we select ike which is used. Under IPsec Proposal, we use test in this example.

Step 8: Look for PFS, we set NONE here, under SA Lifetime, enter “28800” or the period you want. Look for Status then select Activate.

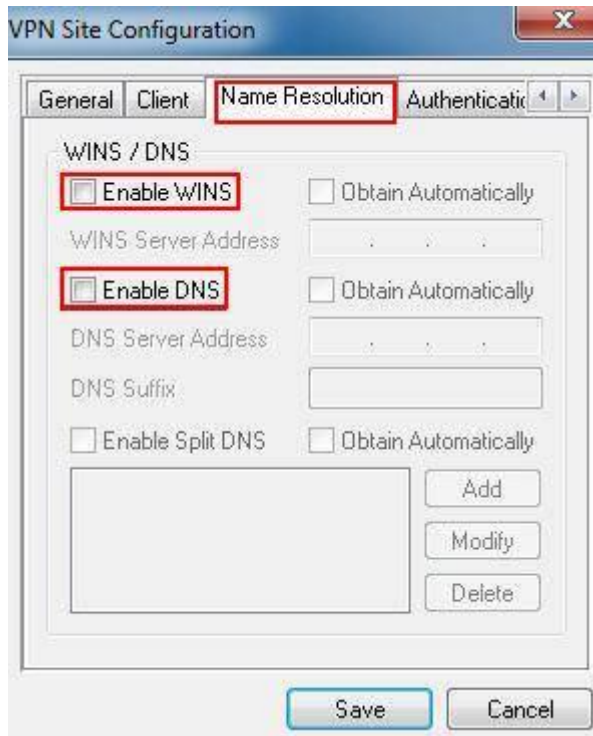
Step 9: Enable IPsec and then click on Add.

C. Configuring the Shrew VPN Client

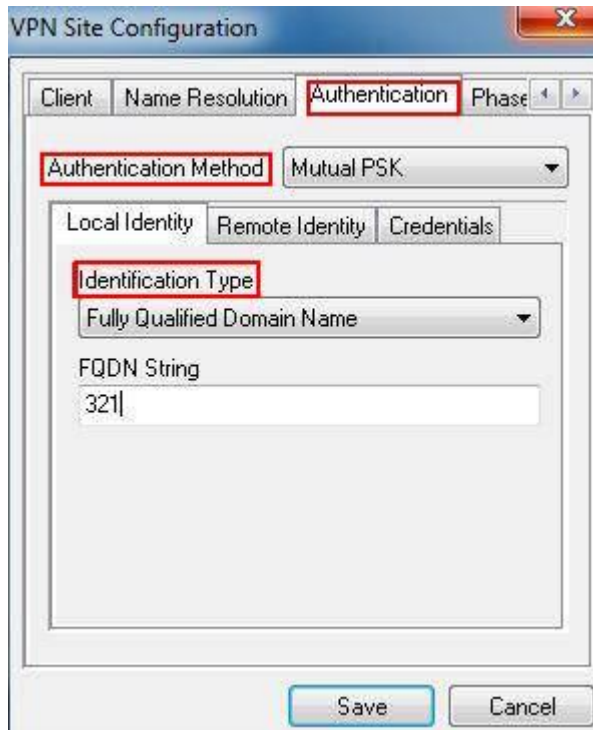
Step 1: Click on Add. Under Host Name or IP Address, enter the TL-ER6120’s WAN IP address, select disable for Auto Configuration. Under Address Method, we select Using an existing adapter and current address.



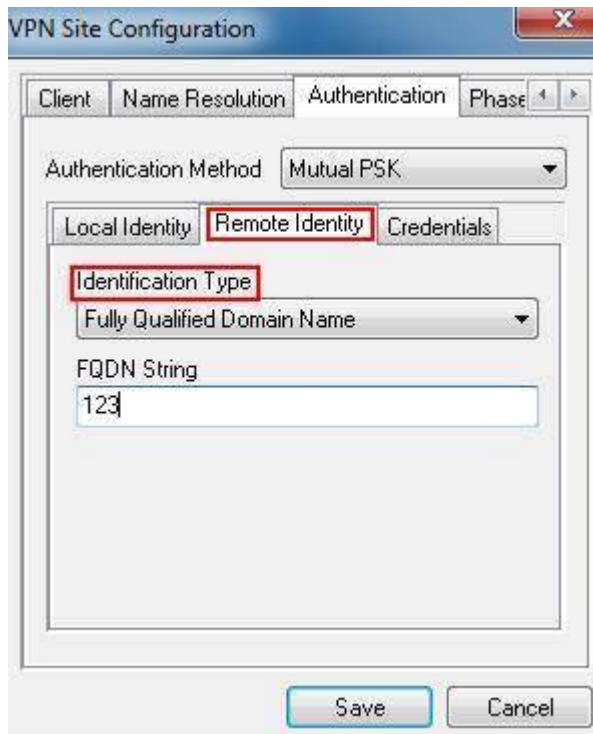
Step 2: Click on Name Resolution on the top menu, don’t tick the Enable WINS and Enable DNS.



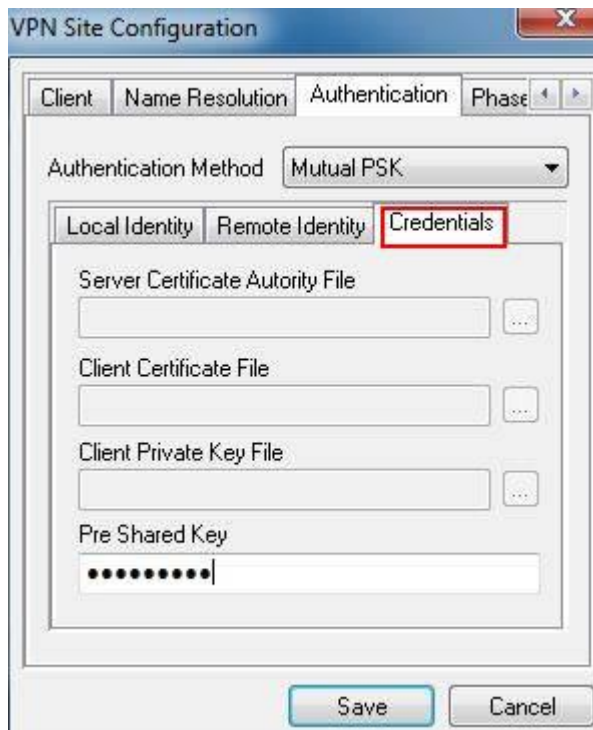
Step 3: Click on Authentication on the top menu, select Mutual PSK as Authentication. Under Identification Type, select Fully Qualified Domain Name and enter "321" for FQDN String.



Step 4: Click on Remote Identity, select Fully Qualified Domain Name as Identification Type and enter "123" for FQDN String.



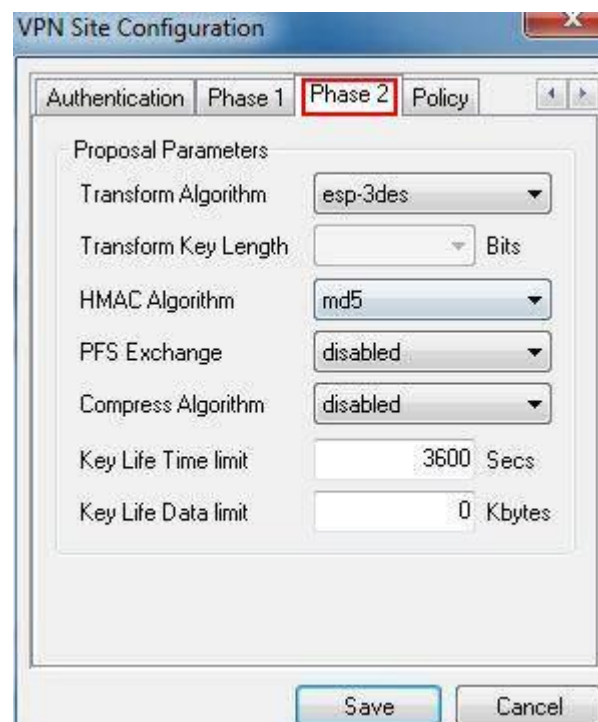
Step 5: Click on Credentials, the Pre Shared Key, should be the same as the Pre-shared Key on the TL-ER6120, it's "123456789".



Step 6: Click on Phase 1, under the Proposal Parameters, the Exchange Type, DH Exchange, Cipher Algorithm, and Hash Algorithm are the same with TL-ER6120's, we use aggressive, group 2, 3des, md5 here.



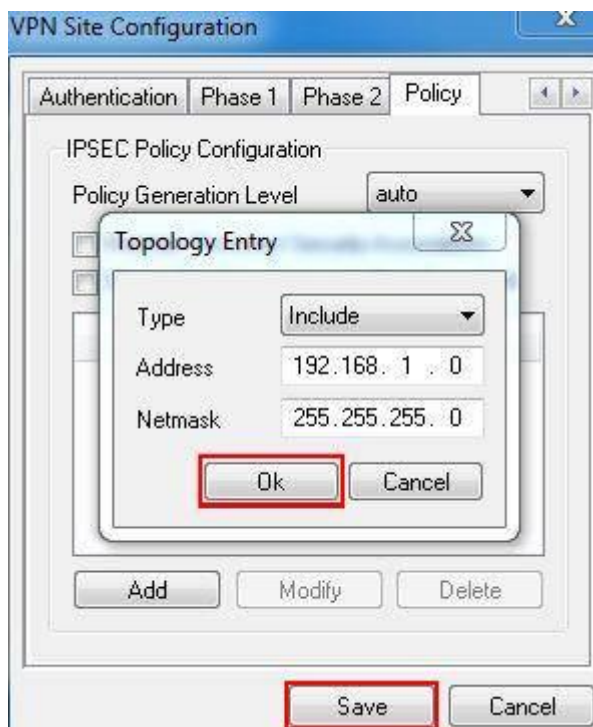
Step 7: Click on Phase 2, under the Proposal Parameters, the Transform Algorithm, HMAC Algorithm are the same with TL-ER6120's we use esp-3des, md5 here. PFS Exchange and Compress Algorithm are disabled.



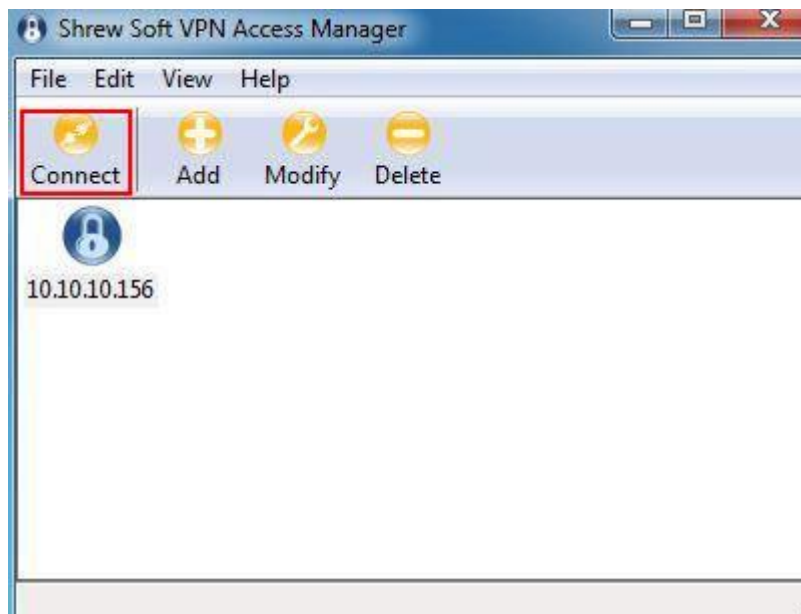
Step 8: Click on Policy, don't tick Obtain Topology Automatically or Tunnel All. Then click on Add.



Step 9: Select Include as Type, enter the TL-ER6120's LAN Subnet Address and Subnet Mask, it's 192.168.1.0, 255.255.255.0. Then click on OK and Save.



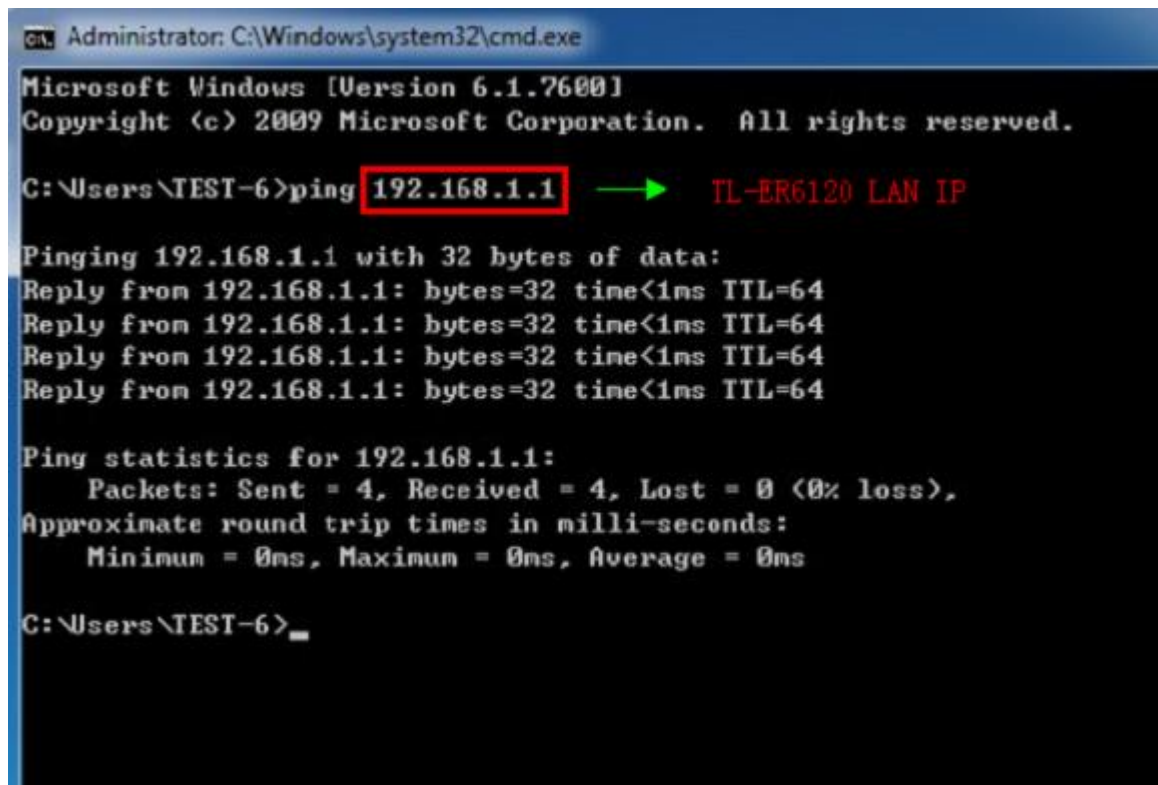
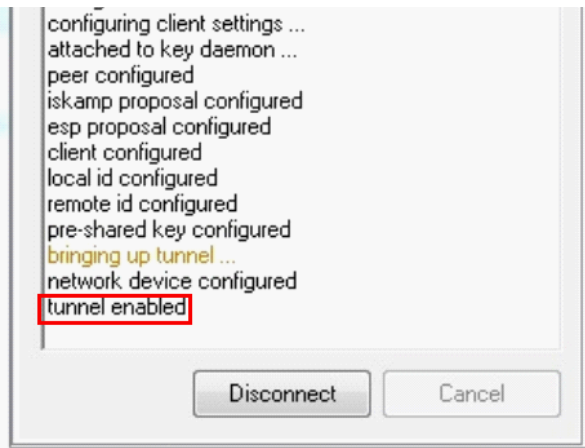
Step 10: Click on Connect.



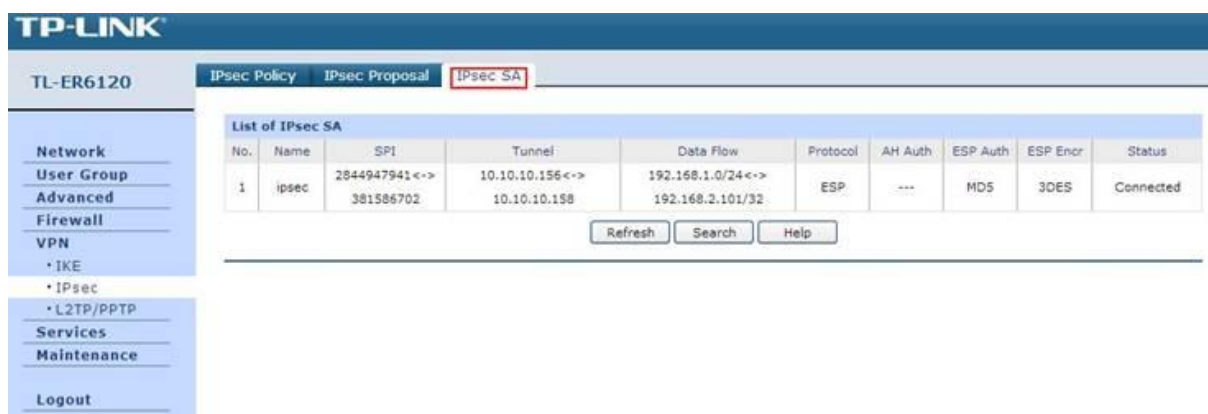
Step 11: Click on Connect.



Step 12: After Shrew Soft VPN show tunnel enabled as the followings, you need ping TL-ER6120 LAN IP.



Step 13: If client connect to the VPN Server successfully, you can see IPsec SA on the list.



5. How to configure LAN-to-LAN L2TP/PPTP VPN on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



LAN-to-LAN L2TP/PPTP VPN connection is established between two VPN routers. To configure LAN-to-LAN L2TP/PPTP VPN on TL-LINK Routers, please follow the instructions below:

- A. Connecting the devices together**
- B. Verify the settings needed for L2TP/PPTP VPN on Router**
- C. Configuring a L2TP/PPTP Server on TP-LINK router(Router A)**
- D. Configuring a L2TP/PPTP Client on TP-LINK router(Router B)**

NOTE: We give the guide to configure LAN-to-LAN PPTP VPN in this example, the way to configure LAN-to-LAN L2TP VPN is similar. If the TP-LINK Router configured as PPTP Server is behind a NAT device, Virtual Server or DMZ should be configured on the NAT device, otherwise the VPN tunnel can't be established.

A. Connecting the devices together

Before setup a VPN tunnel, you need to ensure that the two routers are connected to the Internet. After ensuring that there is an active Internet connection on each router, you need to verify the VPN settings of the two routers, please follow the instruction below.

B. Verify the settings needed for PPTP VPN on Router

Router A's Status Page:

Device Info

Firmware Version:1.0.1 Build 20120417 Rel.62469

Hardware Version:TL-ER6120 v1.0

System Time

System Time:2012-05-17 19:02:34 Thursday

Running Time:26 Min, 16 Sec

WAN

WAN1

Link Up

Primary Connection:PPPoE/Russian PPPoE

Status:Connected

Online Time:1 Min, 55 Sec

IP Address:183.37.240.111

Subnet Mask:255.255.255.255

MAC Address:B0-48-7A-DD-87-EF

Secondary Connection:

Status:

IP Address:

Subnet Mask:---

WAN2

Link Down

Primary Connection:Dynamic IP

Status:Connecting...

IP Address:0.0.0.0

Subnet Mask:0.0.0.0

Gateway:0.0.0.0

MAC Address:B0-48-7A-DD-87-F0

Secondary Connection:---

Status:---

IP Address:---

Subnet Mask:---

This is Router A's IP

This is Router A's local subnet

LAN/DMZ

Interface

IP Address

Subnet Mask

DHCP Server

MAC Address

LAN

192.168.0.1

255.255.255.0

Enabled

B0-48-7A-DD-87-EE

Router B's Status Page:

Device Info

Firmware Version:1.0.1 Build 20120417 Rel.62469

Hardware Version:TL-ER6120 v1.0

System Time

System Time:2012-05-17 19:07:36 Thursday

Running Time:2 Day, 10 Hour, 42 Min, 28 Sec

WAN

WAN1

Link Up

Primary Connection:PPPoE/Russian PPPoE

Status:Connected

Online Time:28 Min, 33 Sec

IP Address:183.16.194.116

Subnet Mask:255.255.255.255

MAC Address:B0-48-7A-DD-8A-0B

Secondary Connection:---

Status:---

IP Address:---

Subnet Mask:---

WAN2

Link Down

Primary Connection:Dynamic IP

Status:Connecting...

IP Address:0.0.0.0

Subnet Mask:0.0.0.0

Gateway:0.0.0.0

MAC Address:B0-48-7A-DD-8A-0C

Secondary Connection:---

Status:---

IP Address:---

Subnet Mask:---

This is Router B's local subnet

LAN/DMZ

Interface

IP Address

Subnet Mask

DHCP Server

MAC Address

LAN

192.168.1.1

255.255.255.0

Enabled

B0-48-7A-DD-8A-0A

C. Configuring a PPTP Server on TP-LINK router

Step 1 : Access Router A's management page, click on VPN->L2TP/PPTP->IP Address Pool, enter Pool Name and IP Address Range, and then click on Add.

Enter pool name

Click on Add

Pool Name: VPN

IP Address Range: 172.31.10.100 - 172.31.10.200

Add

Clear

Help

List of IP Address Pool

| No. | Pool Name | IP Address Range | Action |
|-------------|-----------|------------------|--------|
| No entries. | | | |

Select All Delete Search

NOTE:

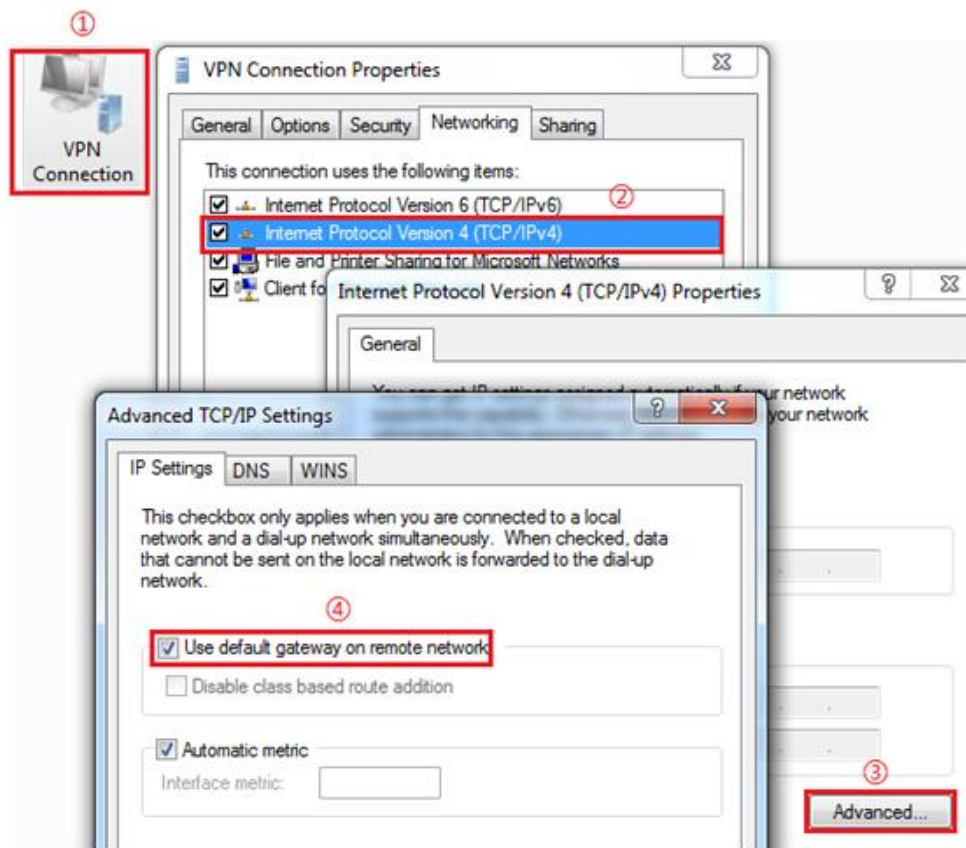
1) The IP addresses in the IP Address Pool can only be in the same subnet with the VPN router's LAN port in the latest firmware, and in the earlier version firmware, IP Address pool must be in the different subnet with the VPN router's LAN IP address range.

2) If the IP addresses in the IP Address Pool is in the same subnet with the VPN router's LAN port, the remote VPN clients can directly access the Internet. It's recommended that the IP address range in the IP Address Pool do not overlap with the one in the local DHCP IP address pool. If not in the same subnet, it must configure an extra multi-nets NAT entry. Only in this way, the remote VPN clients can access the Internet via the VPN router in the headquarters. The following contents will respectively introduce the two situations.

● In the Same Subnet

1) Configure the IP Address Pool of access router A as step 1.

2) Keep using the default gateway on remote network on clients, as the steps in the following picture.



- In the Different Subnet

1) Configure the IP Address Pool of access router A as step 1.

IP Address Pool

Enter pool name

Pool Name: PPTP2_Dialup_User

IP Address Range: 10.10.10.2 - 10.10.10.33

Click on Add

Add

Clear

Help

List of IP Address Pool

| No. | Pool Name | IP Address Range | Action |
|-------------|-----------|------------------|--------|
| No entries. | | | |

Select All Delete Search

2) Choose the menu **Advanced**→**NAT**→**Multi-Nets NAT** to enter the **Subnet/Mask** and select the Status **Activate**.

Multi-Nets NAT

Subnet/Mask: /

Description: (Optional)

Status: ☒ Activate ☐ Inactivate

Click on Add → **Add**

List of Rules

| No. | Network Address | Description | Status | Action |
|-------------|-----------------|-------------|--------|--------|
| No entries. | | | | |

Select All Activate Inactivate Delete Search

3) Keep using the default gateway on remote network on clients.

Step 2 : Go to L2TP/PPTP Tunnel, look for protocol, select PPTP; the Mode should be Server.

L2TP/PPTP Tunnel

IP Address Pool List of L2TP/PPTP Tunnel

DNS setting is not necessary, it can be kept as default

Hello Interval: Sec (60-1000)

Primary DNS: (Only for Server Mode)

Secondary DNS: (Only for Server Mode)

NetBIOS Passthrough: ☒ Enable ☐ Disable

Click on Save → **Save**

L2TP/PPTP Tunnel

Protocol: ☐ L2TP ☒ PPTP

Mode: ☒ Server ☐ Client

Account Name:

Password:

Tunnel: Select LAN-to-LAN

Max Connections: (1-10)

Encryption: ☐ Enable ☒ Disable

Pre-shared Key:

Client IP:

IP Address Pool:

Remote Subnet: / Enter Router B's local subnet

Status: ☒ Activate ☐ Inactivate

Click on Add → **Add**

Step 3 : Enter Account Name and Password whatever you like, here we use "pptp" as account name, password is "pptp".

Step 4 : Under Tunnel, select LAN-to-LAN.

Step 5 : Under IP Address Pool, select "VPN" we have added before.

Step 6 : Under Remote Subnet, enter Router B's local subnet, we enter "192.168.1.0/24" in this example.

Step 7 : Look for Status, select Active.

Step 8 : Click on Add and then click on Save.

Note:

1) If the IP addresses in the IP Address Pool is not in the same subnet with the Router A's LAN port, the IP address Pool here should choose PPTP2_Dialup_User.

2) In the latest firmware of TP-LINK router, the Enable VPN-to-Internet button is removed and the VPN feature is enabled by default.

3) DNS setting is not necessary and it can be kept as default. The default IP is "0.0.0.0", which means the LAN IP of the router is used as the DNS server address. Or you can enter the well-known DNS server.

D. Configuring a PPTP client on TP-LINK Router

Step 1 : Access Router B's management page, go to L2TP/PPTP Tunnel, look for protocol, select PPTP; the Mode should be Client.

Step 2 : Enter "pptp" as Account Name and "pptp" as Password.

L2TP/PPTP Tunnel | IP Address Pool | List of L2TP/PPTP Tunnel

General

Hello Interval: 60 Sec (60-1000)

Primary DNS: 0.0.0.0 (Only for Server Mode)

Secondary DNS: 0.0.0.0 (Only for Server Mode)

NetBIOS Passthrough: ☒ Enable ☐ Disable

L2TP/PPTP Tunnel

Protocol: ☐ L2TP ☒ PPTP

Mode: ☐ Server ☒ Client

Account Name: pptp

Password: ****

WAN: WAN1

Server IP: 183.37.240.111 (IP address / Domain name)

Encryption: ☐ Enable ☒ Disable

Pre-shared Key:

Client IP:

IP Address Pool:

Remote Subnet: 192.168.0.0 / 24

Status: ☒ Activate ☐ Inactivate

Click on Save

Click on Add

Enter Account Name and Password

Enter Router A's IP

Enter Router A's local subnet

Save

Add

Clear

Help

Step 3 : Under Server IP, enter Router A's IP address, which is 183.37.240.111.

Step 4 : Under Remote Subnet, enter Router B's local subnet, we enter "192.168.1.0/24" in this example.

Step 5 : Look for Status, select Active.

Step 6 : Click on Add and then click on Save.

Step 7: If the PPTP tunnel is established successfully, you can check it on List of Tunnel.

| L2TP/PPTP Tunnel IP Address Pool List of L2TP/PPTP Tunnel | | | | | | | | | |
|---|----------|---------|--------|-----------|------------|----------------|---------------------------|-----------|---|
| List of Tunnel | | | | | | | | | |
| No. | Protocol | Account | Mode | Tunnel ID | Session ID | Peer IP | Peer Name | Status | Action |
| 1 | PPTP | pptp | Client | 0,0 | 2,1 | 183.37.240.111 | TP-LINK_SMB_ TL-ER6120 | Connected |  |
| <div>Refresh Search Help</div> | | | | | | | | | |

Also, PC within the local subnet of Router B, can ping Router A's LAN IP (192.168.0.1).

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\TEST>ping 192.168.0.1

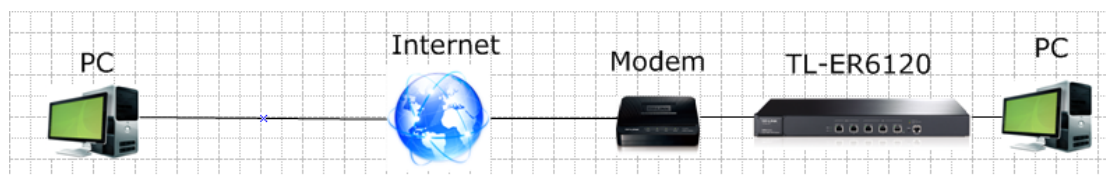
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=36ms TTL=63
Reply from 192.168.0.1: bytes=32 time=37ms TTL=63
Reply from 192.168.0.1: bytes=32 time=36ms TTL=63
Reply from 192.168.0.1: bytes=32 time=37ms TTL=63

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 36ms, Maximum = 37ms, Average = 36ms

C:\Users\TEST>
```

6. How to configure a PPTP Server on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



PPTP (Point to Point Tunneling Protocol) Server is used to create a VPN connection for remote clients. To configure PPTP Server on TP-LINK router, please follow the instructions below:

- A. Make sure PCs of two sides can access to Internet**
- B. Configuring a PPTP Server on TP-LINK router**
- C. Configuring PPTP client on remote PC (Windows 7)**

NOTE: If the TP-LINK Router is behind a NAT device, Virtual Server or DMZ should be configured on the NAT device, otherwise the VPN tunnel can't be established.

A. Make sure PCs of two sides can access to Internet

Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring a PPTP Server on TP-LINK router

Step 1:

Access the router's management webpage, verify the settings needed on the router.

| Device Info | |
|-------------------|--------------------------------|
| Firmware Version: | 1.0.0 Build 20111114 Rel.52682 |
| Hardware Version: | TL-ER6120 v1.0 |

| System Time | |
|---------------|----------------------------|
| System Time: | 2012-03-02 10:09:08 Friday |
| Running Time: | 1 Hour, 25 Min, 15 Sec |

| WAN | |
|-----------------------|---------------------|
| WAN1 | Link Up |
| Primary Connection: | PPPoE/Russian PPPoE |
| Status: | Connected |
| Online Time: | 9 Min, 37 Sec |
| IP Address: | 218.18.1.74 |
| Subnet Mask: | 255.255.255.255 |
| MAC Address: | 90-F6-52-49-A0-67 |
| Secondary Connection: | --- |
| Status: | --- |
| IP Address: | --- |
| Subnet Mask: | --- |
| WAN2 | Link Down |
| Primary Connection: | Dynamic IP |
| Status: | Connecting... |
| IP Address: | 0.0.0.0 |
| Subnet Mask: | 0.0.0.0 |
| Gateway: | 0.0.0.0 |
| MAC Address: | 90-F6-52-49-A0-68 |
| Secondary Connection: | --- |
| Status: | --- |
| IP Address: | --- |
| Subnet Mask: | --- |

| LAN/DMZ | | | | |
|-----------|-------------|---------------|-------------|-------------------|
| Interface | IP Address | Subnet Mask | DHCP Server | MAC Address |
| LAN | 192.168.0.1 | 255.255.255.0 | Enabled | 90-F6-52-49-A0-66 |

Step 2:

Click on VPN->L2TP/PPTP->IP Address Pool, enter Pool Name and IP Address Range, and then click on Add.

| TP-LINK | | | | | | | | | | | | |
|--|-----------|------------------|--------|--|-----|-----------|------------------|--------|-------------|--|--|--|
| TL-ER6120 | | | | | | | | | | | | |
| L2TP/PPTP Tunnel IP Address Pool List of L2TP/PPTP Tunnel | | | | | | | | | | | | |
| <div> <div> <div>Network</div> <div>User Group</div> <div>Advanced</div> <div>Firewall</div> <div>VPN</div> <div>• IKE</div> <div>• IPsec</div> <div>• L2TP/PPTP</div> <div>Services</div> <div>Maintenance</div> </div> <div> <div>IP Address Pool</div> <div> <div>Enter Pool Name</div> <div>Pool Name: <input type="text" value="group"/></div> <div>IP Address Range: <input type="text" value="172.31.10.10"/> - <input type="text" value="172.31.10.50"/></div> <div>Click on Add</div> <div> <div>Add</div> <div>Clear</div> <div>Help</div> </div> </div> </div> </div> | | | | | | | | | | | | |
| <div> <div>List of IP Address Pool</div> <table border="1"> <thead> <tr> <th>No.</th> <th>Pool Name</th> <th>IP Address Range</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="4">No entries.</td> </tr> </tbody> </table> <div> <div>Select All</div> <div>Delete</div> <div>Search</div> </div> </div> | | | | | No. | Pool Name | IP Address Range | Action | No entries. | | | |
| No. | Pool Name | IP Address Range | Action | | | | | | | | | |
| No entries. | | | | | | | | | | | | |

NOTE:

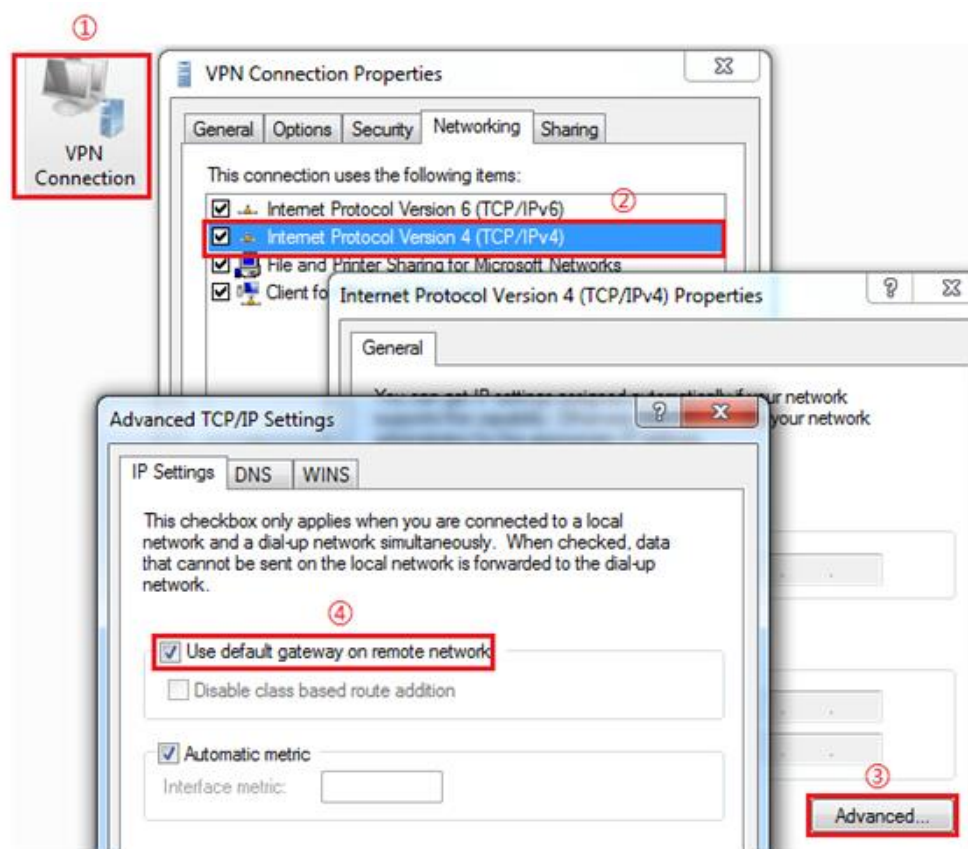
1) The IP addresses in the IP Address Pool can only be in the same subnet with the VPN router's LAN port in the latest firmware, and in the earlier version firmware, IP Address pool must be in the different subnet with the VPN router's LAN IP address range.

2) If the IP addresses in the IP Address Pool is in the same subnet with the VPN router's LAN port, the remote VPN clients can directly access the Internet. It's recommended that the IP address range in the IP Address Pool do not overlap with the one in the local DHCP IP address pool. If not in the same subnet, it must configure an extra multi-nets NAT entry. Only in this way, the remote VPN clients can access the Internet via the VPN router in the headquarters. The following contents will respectively introduce the two situations.

- In the Same Subnet

1) Configure the IP Address Pool of access router A as step 2.

2) Keep using the default gateway on remote network on clients, as the steps in the following picture.



- In the Different Subnet

1) Configure the IP Address Pool of access router A as step 1.

Enter pool name

IP Address Pool

Pool Name:

IP Address Range: -

Click on Add → **Add**

Clear
Help

List of IP Address Pool

| No. | Pool Name | IP Address Range | Action |
|-------------|-----------|------------------|--------|
| No entries. | | | |

Select All Delete Search

2) Choose the menu **Advanced**→**NAT**→**Multi-Nets NAT** to enter the **Subnet/Mask** and select the Status **Activate**.

Multi-Nets NAT

Subnet/Mask: /

Description: (Optional)

Status: ☒ Activate ☐ Inactivate

Click on Add → **Add**

Clear
Help

List of Rules

| No. | Network Address | Description | Status | Action |
|-------------|-----------------|-------------|--------|--------|
| No entries. | | | | |

Select All Activate Inactivate Delete Search

3) Keep using the default gateway on remote network on clients.

Step 3:

Look for protocol, select PPTP; the Mode should be Server.

The screenshot shows the 'L2TP/PPTP Tunnel' configuration window. At the top, there are tabs: 'L2TP/PPTP Tunnel' (selected), 'IP Address Pool', and 'List of L2TP/PPTP Tunnel'. Below the tabs, there are two main sections. The first section, titled 'General', contains fields for 'Hello Interval' (set to 60), 'Primary DNS' (0.0.0.0), 'Secondary DNS' (0.0.0.0), and 'NetBIOS Passthrough' (set to Enable). A green callout box points to the DNS fields with the text 'DNS setting is not necessary, it can be kept as default'. A green arrow points from the 'Save' button to the text 'Click on Save'. The second section, titled 'L2TP/PPTP Tunnel', contains fields for 'Protocol' (PPTP selected), 'Mode' (Server selected), 'Account Name' (client), 'Password' (masked with dots), 'Tunnel' (Client-to-LAN selected), 'Max Connections' (5), 'Encryption' (Disable selected), 'Pre-shared Key', 'Client IP', 'IP Address Pool' (Group selected), 'Remote Subnet', and 'Status' (Activate selected). A green callout box points to the 'Account Name' and 'Password' fields with the text 'Enter Account Name and Password'. A green arrow points from the 'Add' button to the text 'Click on Add'.

Step 4:

Enter Account Name and Password whatever you like, here we use “client” as account name, password is “123456”.

Step 5:

Under Tunnel, select Client-to-LAN.

Step 6:

The tunnel supports up to 10 connections, we enter 5 in this example.

Step 7:

Under IP Address Pool, select “group” we have added before.

Step 8:

Look for Status, select Active.

Step 9:

Click on Add and then click on Save.

Note:

1) If the IP addresses in the IP Address Pool is not in the same subnet with the VPN router's LAN port, the IP address Pool here should choose PPTP2_Dialup_User.

2) In the latest firmware of TP-LINK router, the Enable VPN-to-Internet button is removed and the VPN feature is enabled by default.

3) DNS setting is not necessary and it can be kept as default. The default IP is "0.0.0.0", which means the LAN IP of the router is used as the DNS server address. Or you can enter the well-known DNS server.

C. Configuring PPTP client on remote PC (Windows 7)

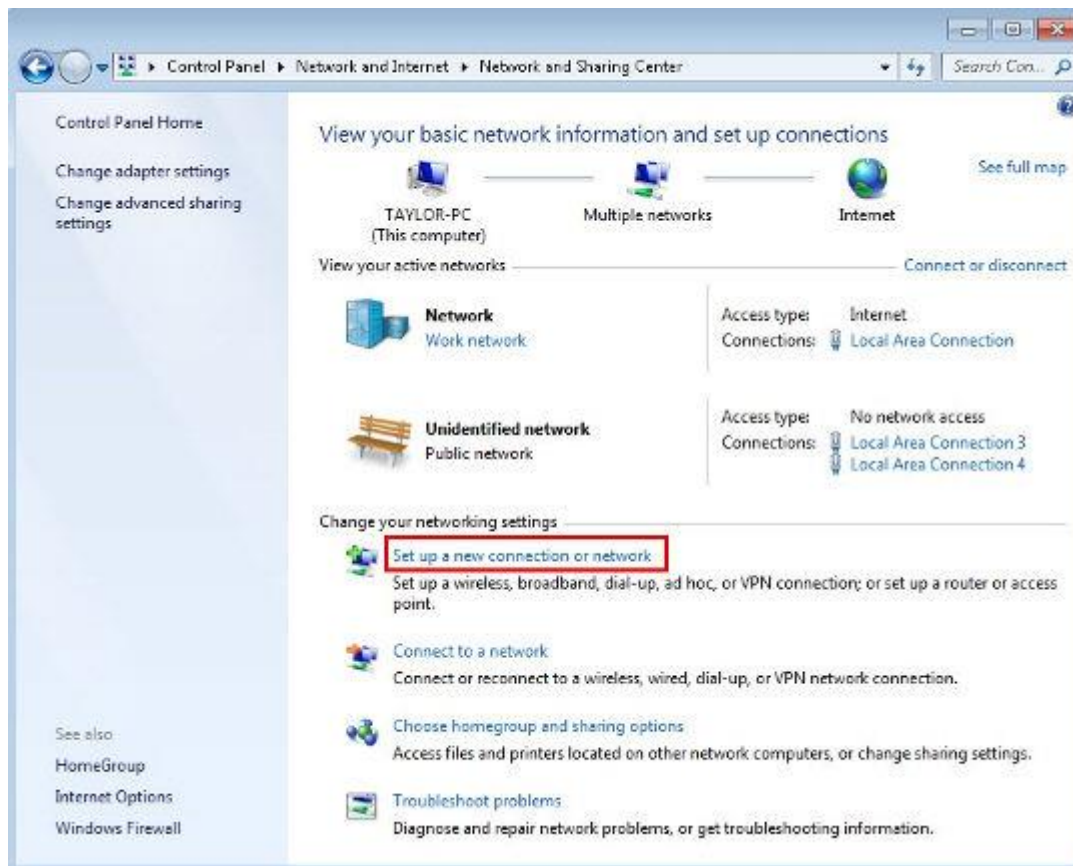
NOTE: For remote PC to connect to PPTP server, it can use Windows built-in PPTP software or Third-party PPTP software.

Step 1:

Click on Start->Control Panel->Network and Internet->Network and Sharing Center.

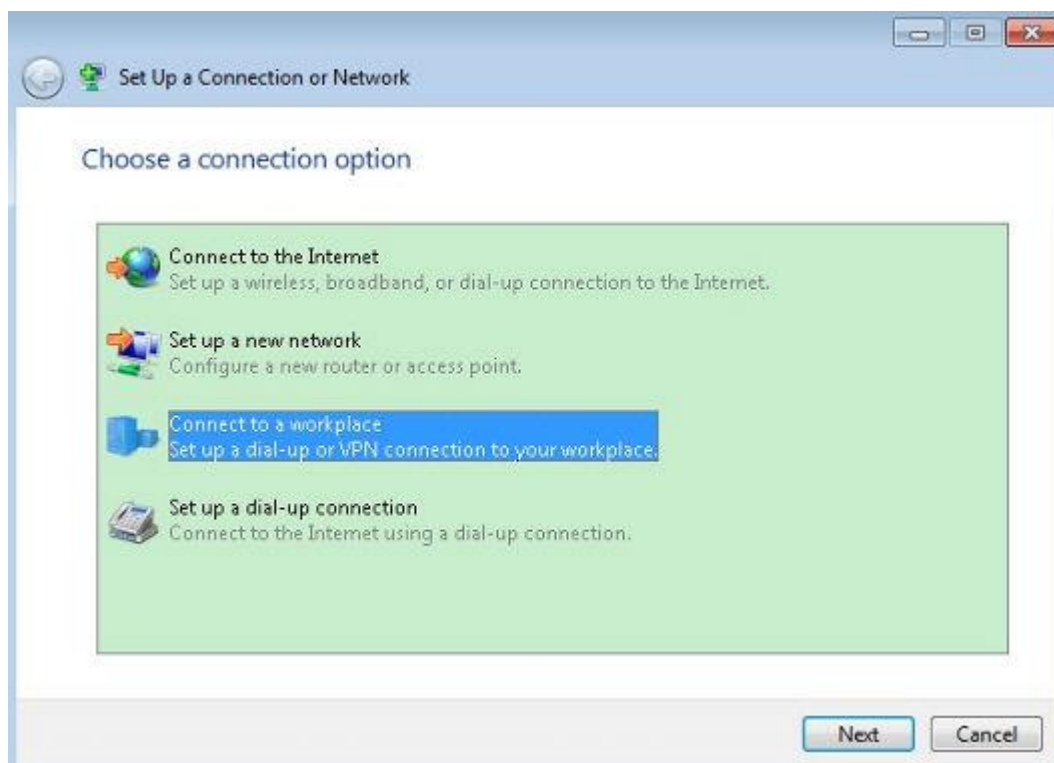
Step 2:

Click on Set up a new connection or network.



Step 3:

Choose Connect to a workplace, and then click on Next.



Step 4:

Select Use my Internet connection (VPN)



Step 5:

Under Internet address field, enter router's WAN IP address, and then click on Next.

Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 218.18.1.74

Destination name: VPN Connection

☐ Use a smart card

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

☒ Don't connect now; just set it up so I can connect later

Next Cancel

Step 6:

Enter User name and Password, and then click on Create.

Connect to a Workplace

Type your user name and password

User name: client

Password: *****

☐ Show characters

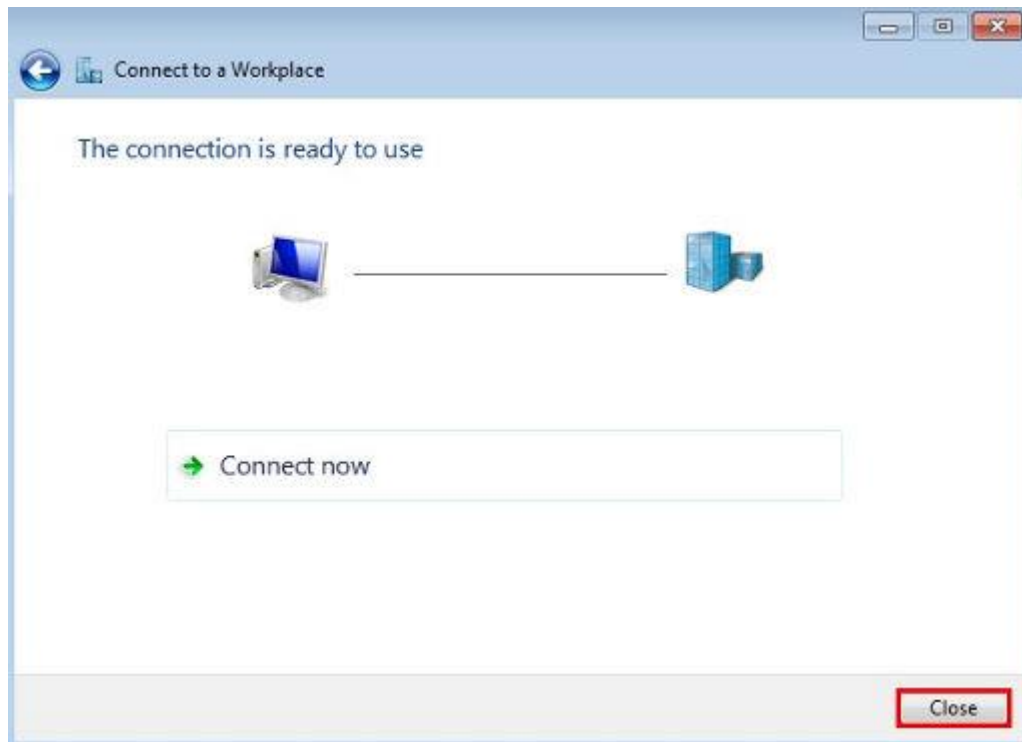
☐ Remember this password

Domain (optional):

Create Cancel

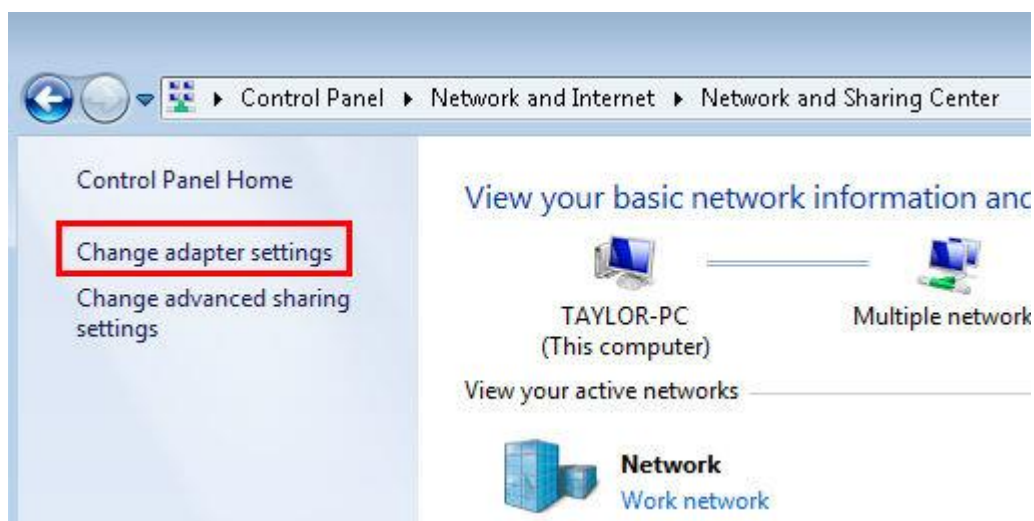
Step 7:

The VPN connection is created and ready to use, click on Close.



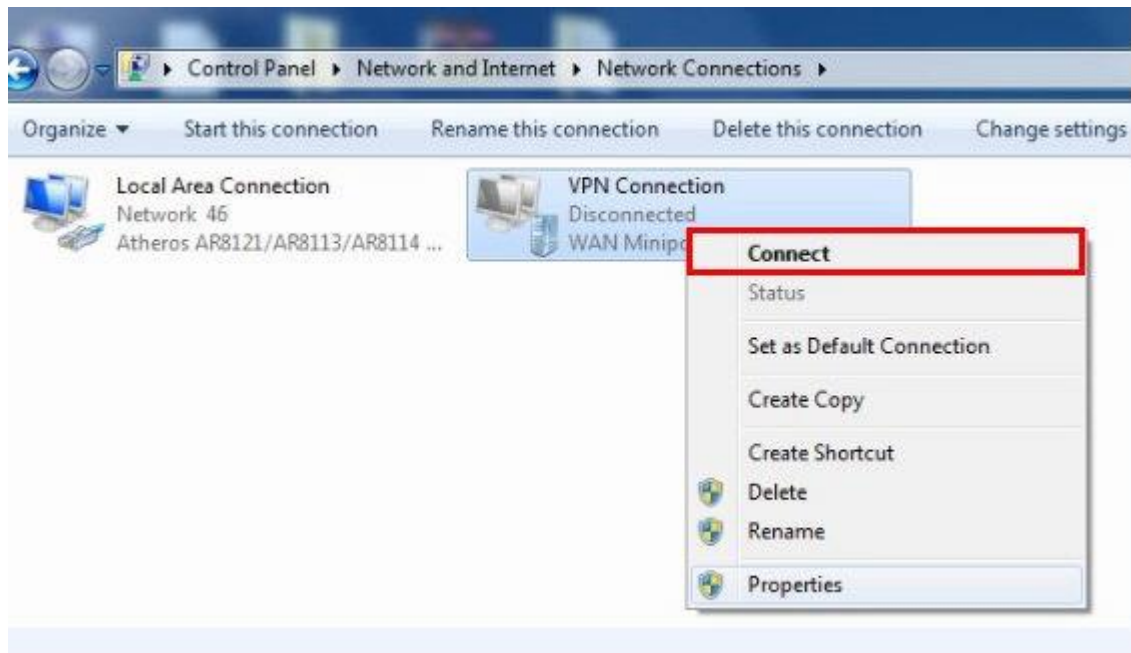
Step 8:

Go to Network and Sharing Center and click on Change adapter settings on the left menu.



Step 9:

Right Click on VPN Connection and select Connect.



Step 10:

Enter User name and Password and then click on Connect.



Step 11:

If the PPTP tunnel is established successfully, you can check it on List of Tunnel.

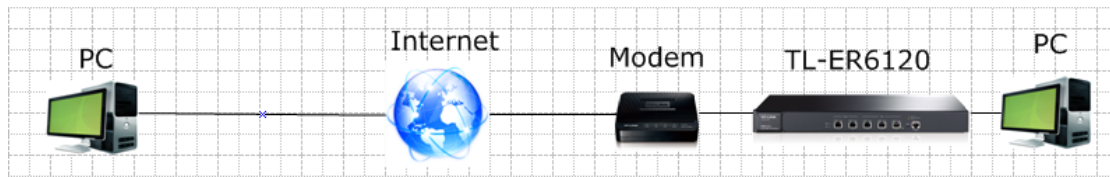
The screenshot displays the TP-LINK TL-ER6120 web management interface. The left sidebar contains a menu with the following items: Network, User Group, Advanced, Firewall, VPN, and L2TP/PPTP. The main content area has three tabs: L2TP/PPTP Tunnel, IP Address Pool, and List of L2TP/PPTP Tunnel. The 'List of L2TP/PPTP Tunnel' tab is active, showing a table with the following data:

| No. | Protocol | Account | Mode | Tunnel ID | Session ID | Peer IP | Peer Name | Status | Action |
|-----|----------|---------|--------|-----------|------------|--------------|-----------|-----------|--------|
| 1 | PPTP | client | Server | 0,0 | 20,1028 | 218.18.0.222 | --- | Connected | |

Below the table, there are three buttons: Refresh, Search, and Help.

7. How to configure a L2TP Server on TP-LINK Router

Suitable for: TL-ER6120, TL-ER6020, TL-ER604W



L2TP (Layer 2 Tunneling Protocol) Server is used to create a VPN connection for remote clients. To configure L2TP Server on TP-LINK router, please follow the instructions below:

- A. Make sure PCs of two sides can access to Internet**
- B. Configuring a L2TP Server on TP-LINK router**
- C. Configuring L2TP client on remote PC (Windows 7)**

NOTE: If the TP-LINK Router is behind a NAT device, Virtual Server or DMZ should be configured on the NAT device, otherwise the VPN tunnel can't be established.

A. Make sure PCs of two sides can access to Internet

Before setup a VPN tunnel, you need to ensure that PCs of two sides are connected to the Internet. After ensuring that there is an active Internet connection on each side, you need to verify the VPN settings of the two sides, please follow the instruction below.

B. Configuring a L2TP Server on TP-LINK router

Step 1:

Access the router's management web page; verify the settings needed on the router.

| Device Info | |
|-------------------|--------------------------------|
| Firmware Version: | 1.0.0 Build 20111114 Rel.52682 |
| Hardware Version: | TL-ER6120 v1.0 |

| System Time | |
|---------------|-------------------------------|
| System Time: | 2012-07-18 10:29:36 Wednesday |
| Running Time: | 4 Day, 22 Hour, 3 Min, 52 Sec |

| WAN | |
|-----------------------|---------------------|
| WAN1 | Link Up |
| Primary Connection: | PPPoE/Russian PPPoE |
| Status: | Connected |
| Online Time: | 3 Sec |
| IP Address: | 113.97.237.50 |
| Subnet Mask: | 255.255.255.255 |
| MAC Address: | 90-F6-52-BD-EE-FB |
| Secondary Connection: | --- |
| Status: | --- |
| IP Address: | --- |
| Subnet Mask: | --- |
| WAN2 | Link Down |
| Primary Connection: | Dynamic IP |
| Status: | Connecting... |
| IP Address: | 0.0.0.0 |
| Subnet Mask: | 0.0.0.0 |
| MAC Address: | 90-F6-52-BD-EE-FC |
| Secondary Connection: | --- |
| Status: | --- |
| IP Address: | --- |
| Subnet Mask: | --- |

| LAN/DMZ | | | | |
|-----------|-------------|---------------|-------------|-------------------|
| Interface | IP Address | Subnet Mask | DHCP Server | MAC Address |
| LAN | 192.168.0.1 | 255.255.255.0 | Enabled | 90-F6-52-BD-EE-FA |

This IP address should be typed in VPN client

Step 2:

Click on VPN->L2TP/PPTP->IP Address Pool, enter Pool Name and IP Address Range, and then click on Add.

| TP-LINK | | | | | | | | | |
|---|---|------------------|-----------|------------------|--------|-------------|--|--|--|
| TL-ER6120 | L2TP/PPTP Tunnel IP Address Pool List of L2TP/PPTP Tunnel | | | | | | | | |
| <ul style="list-style-type: none"> Network User Group Advanced Firewall VPN <ul style="list-style-type: none"> • IKE • IPsec • L2TP/PPTP Services | <p>Enter Pool Name</p> <p>Pool Name: test1</p> <p>IP Address Range: 172.31.10.10 - 172.31.10.20</p> <p>Click on Add</p> <p>Add Clear Help</p> <p>List of IP Address Pool</p> <table border="1"> <thead> <tr> <th>No.</th> <th>Pool Name</th> <th>IP Address Range</th> <th>Action</th> </tr> </thead> <tbody> <tr> <td colspan="4">No entries.</td> </tr> </tbody> </table> <p>Select All Delete Search</p> | No. | Pool Name | IP Address Range | Action | No entries. | | | |
| No. | Pool Name | IP Address Range | Action | | | | | | |
| No entries. | | | | | | | | | |

NOTE:

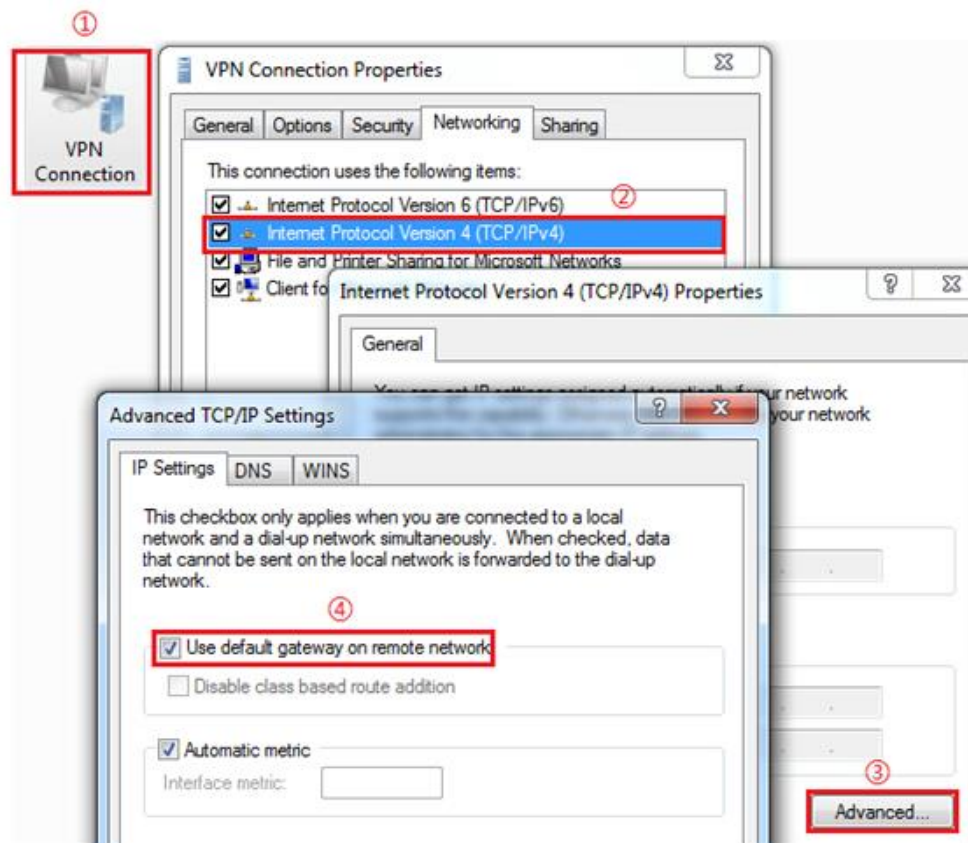
- 1) The IP addresses in the IP Address Pool can only be in the same subnet with the VPN router's LAN port in the latest firmware, and in the earlier version firmware, IP Address pool must be in the different subnet with the VPN router's LAN IP address range.
- 2) If the IP addresses in the IP Address Pool is in the same subnet with the VPN router's LAN port, the remote VPN clients can directly access the Internet. It's recommended that the IP address range in the IP Address Pool do not overlap with the one in the local DHCP IP address pool. If not in the same subnet, it must configure an extra multi-nets NAT entry.

Only in this way, the remote VPN clients can access the Internet via the VPN router in the headquarters. The following contents will respectively introduce the two situations.

- In the Same Subnet

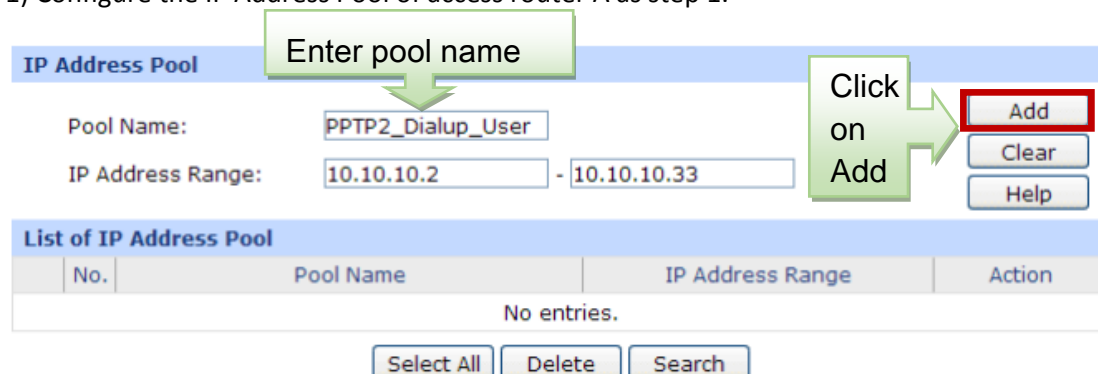
1) Configure the IP Address Pool of access router A as step 2.

2) Keep using the default gateway on remote network on clients, as the steps in the following picture.



- In the Different Subnet

1) Configure the IP Address Pool of access router A as step 1.



2) Choose the menu **Advanced**→**NAT**→**Multi-Nets NAT** to enter the **Subnet/Mask** and select the Status **Activate**.

Multi-Nets NAT

Subnet/Mask: /

Description: (Optional)

Status: ☒ Activate ☐ Inactivate

Click on Add → **Add**

List of Rules

| No. | Network Address | Description | Status | Action |
|-------------|-----------------|-------------|--------|--------|
| No entries. | | | | |

Select All Activate Inactivate Delete Search

3) Keep using the default gateway on remote network on clients.

Step 3:

Look for protocol, select L2TP; the Mode should be Server.

L2TP/PPTP Tunnel | IP Address Pool | List of L2TP/PPTP Tunnel

Get → **DNS setting is not necessary, it can be kept as default**

Hello Interval: Sec (60-1000)

Primary DNS: (Only for Server Mode)

Secondary DNS: (Only for Server Mode)

NetBIOS Passthrough: ☒ Enable ☐ Disable

Click on Save → **Save**

L2TP/PPTP Tunnel

Protocol: ☒ L2TP ☐ PPTP

Mode: ☒ Server ☐ Client

Account Name:

Password:

Tunnel: ▼

Max Connections: (1-10)

Encryption: ☒ Enable ☐ Disable

Pre-shared Key:

Client IP:

IP Address Pool: ▼

Remote Subnet: /

Status: ☒ Activate ☐ Inactivate

Enter Account Name and Password →

Click on Add → **Add**

Step 4:

Enter Account Name and Password whatever you like, here we use “tplinktest” as account name, password is “1234”.

Step 5:

Under Tunnel, select Client-to-LAN.

Step 6:

The tunnel supports up to 10 connections, we enter 10 in this example.

Step 7:

Under Encryption, select Enable, and then enter "5678" as Pre-shared Key.

Step 8:

Under IP Address Pool, select "test1" we have added before.

Step 9:

Look for Status, select Active.

Step 10:

Click on Add.

Note:

1) If the IP addresses in the IP Address Pool is not in the same subnet with the VPN router's LAN port, the IP address Pool here should choose PPTP2_Dialup_User.

2) In the latest firmware of TP-LINK router, the Enable VPN-to-Internet button is removed and the VPN feature is enabled by default.

3) DNS setting is not necessary and it can be kept as default. The default IP is "0.0.0.0", which means the LAN IP of the router is used as the DNS server address. Or you can enter the well-known DNS server.

Step 11:

As we enabled Encryption, we need to go to VPN->IPsec, enable IPsec and then click on Save.



C. Configuring L2TP client on remote PC (Windows 7)

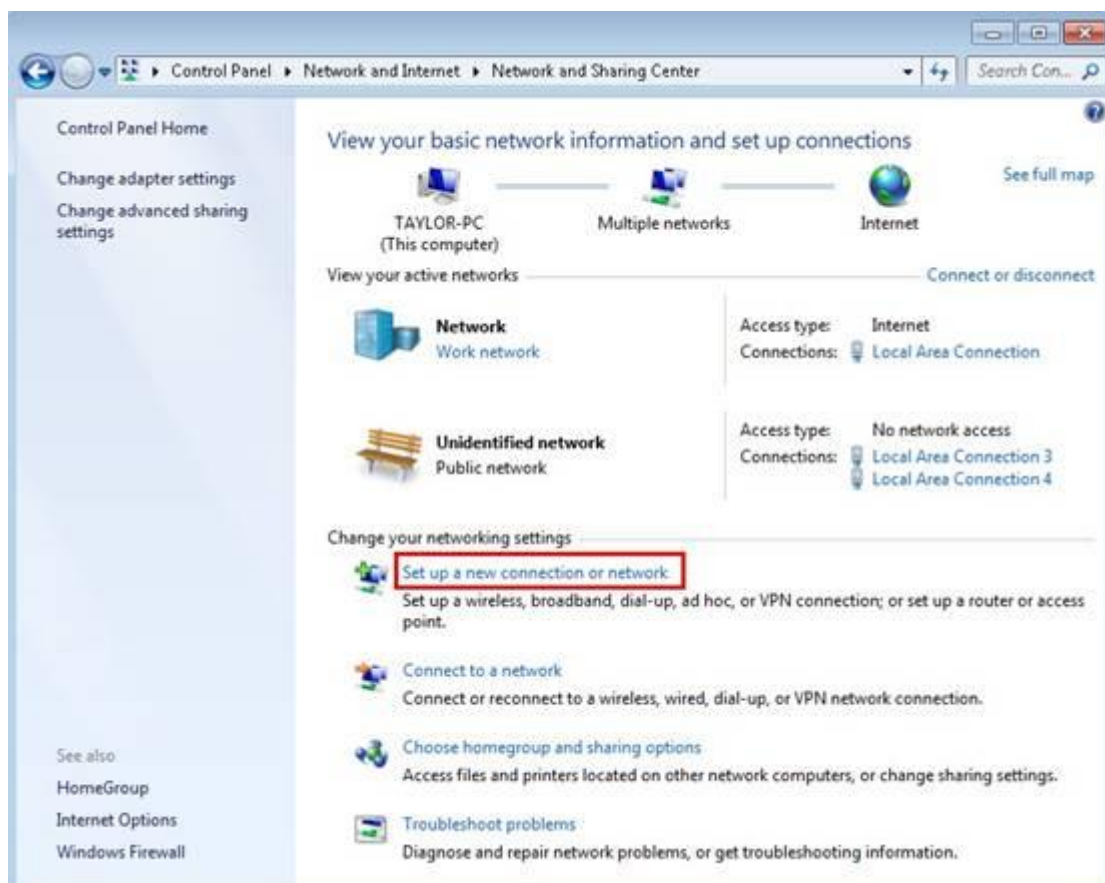
NOTE: For remote PC to connect to L2TP server, it can use Windows built-in L2TP software or Third-party L2TP software.

Step 1:

Click on Start->Control Panel->Network and Internet->Network and Sharing Center.

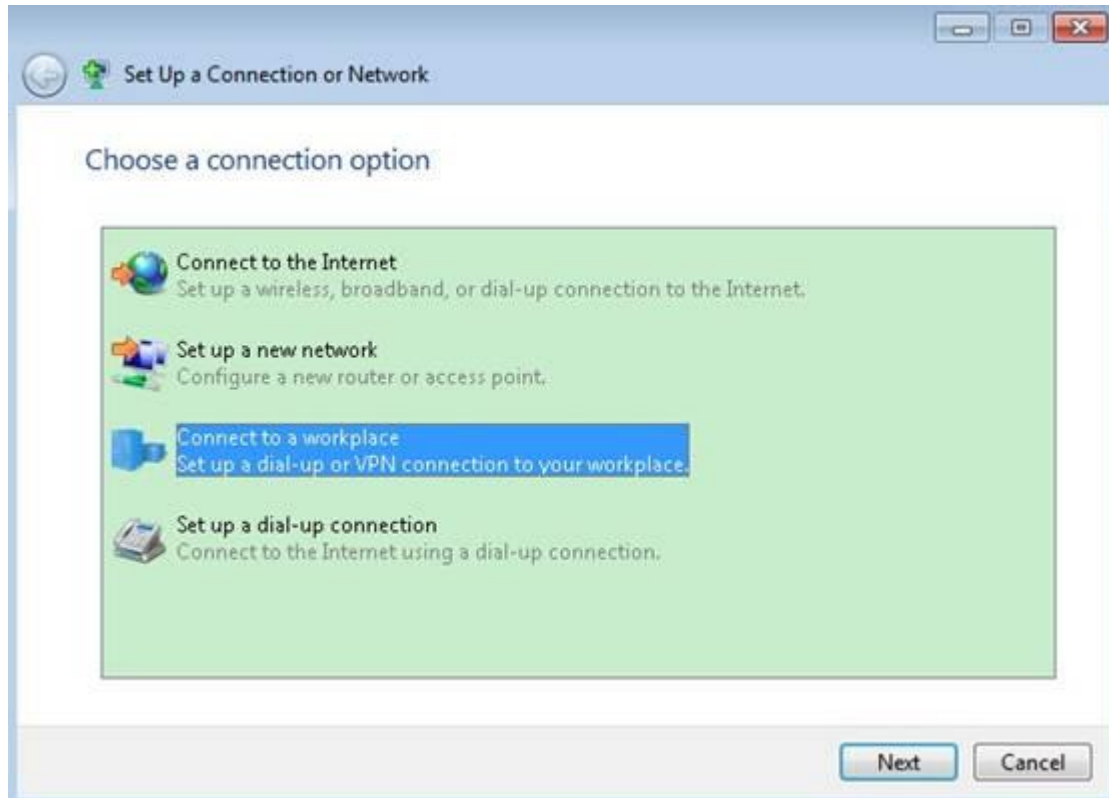
Step 2:

Click on Set up a new connection or network.



Step 3:

Choose Connect to a workplace, and then click on Next.



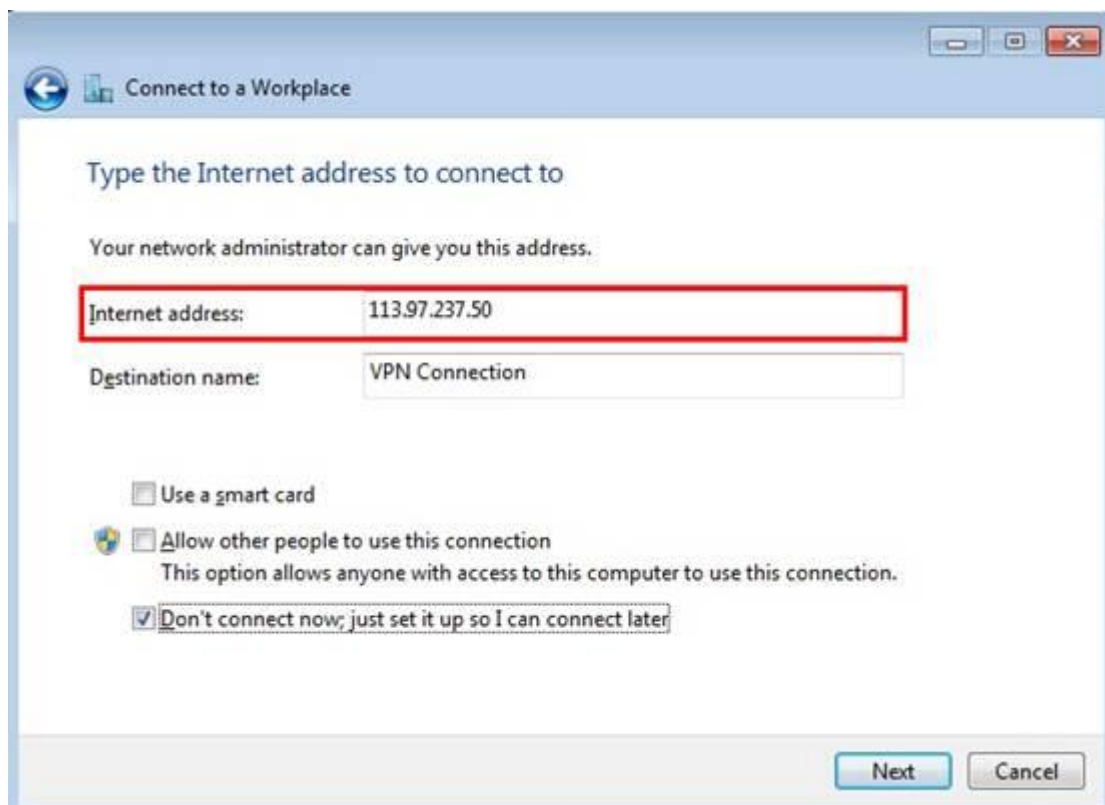
Step 4:

Select Use my Internet connection (VPN)



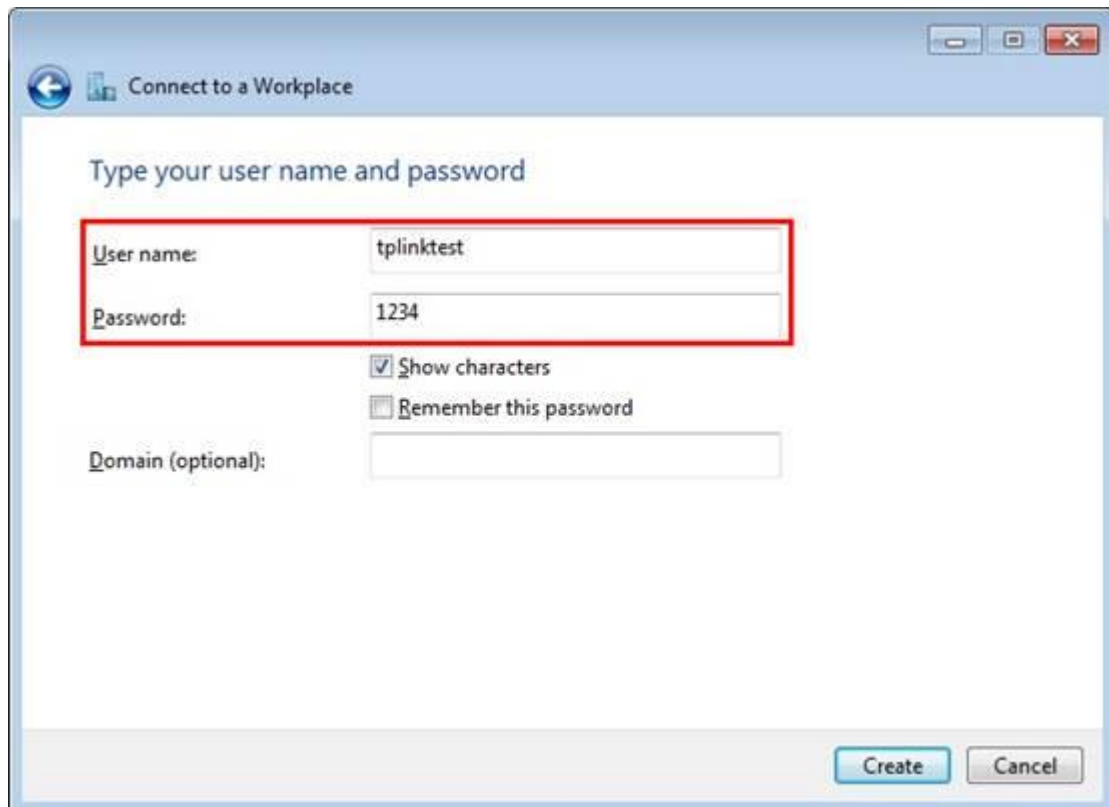
Step 5:

Under Internet address field, enter router's WAN IP address, and then click on Next.



Step 6:

Enter User name and Password, and then click on Create.



Connect to a Workplace

Type your user name and password

User name: tplinktest

Password: 1234

☒ Show characters

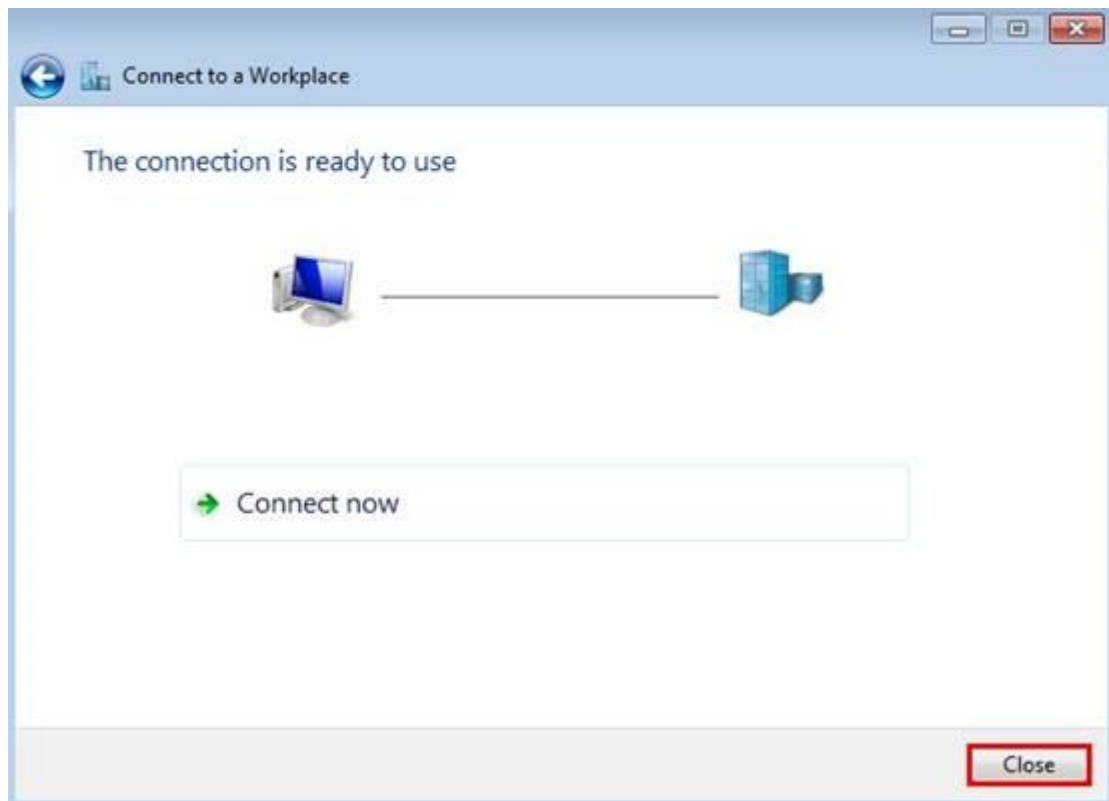
☐ Remember this password

Domain (optional):

Create Cancel

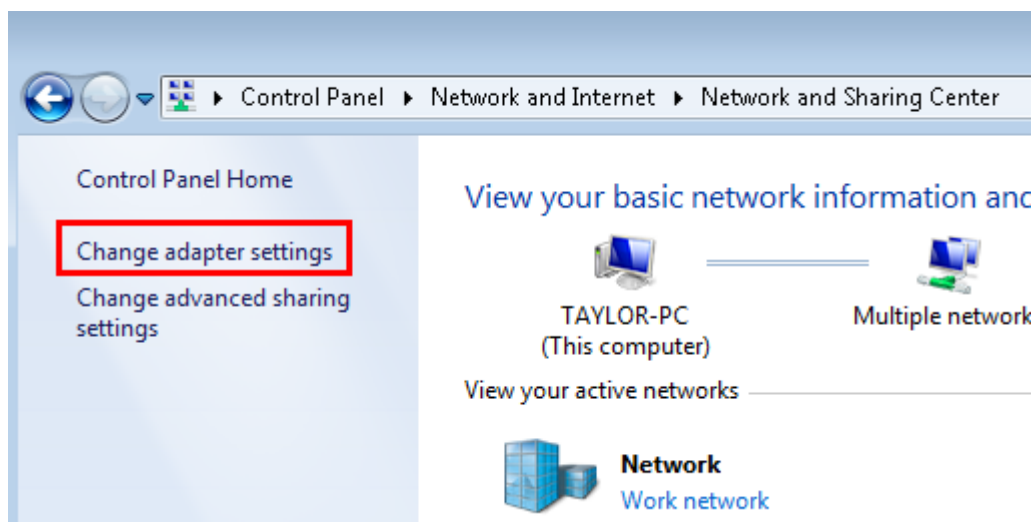
Step 7:

The VPN connection is created and ready to use, click on Close.



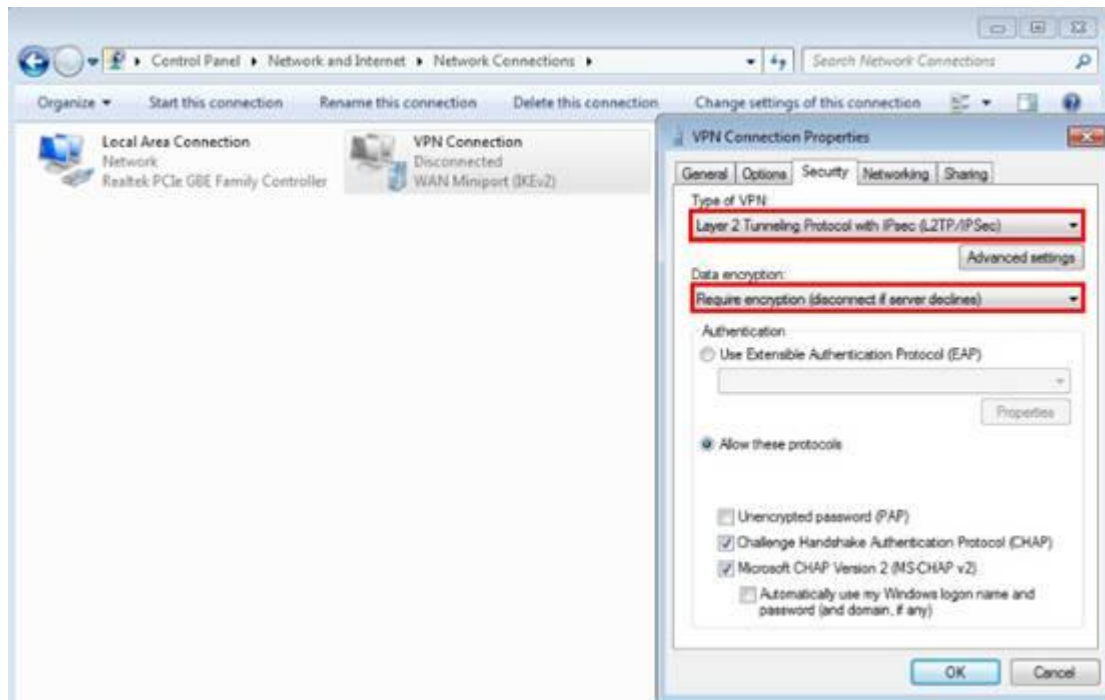
Step 8:

Go to Network and Sharing Center and click on Change adapter settings on the left menu.



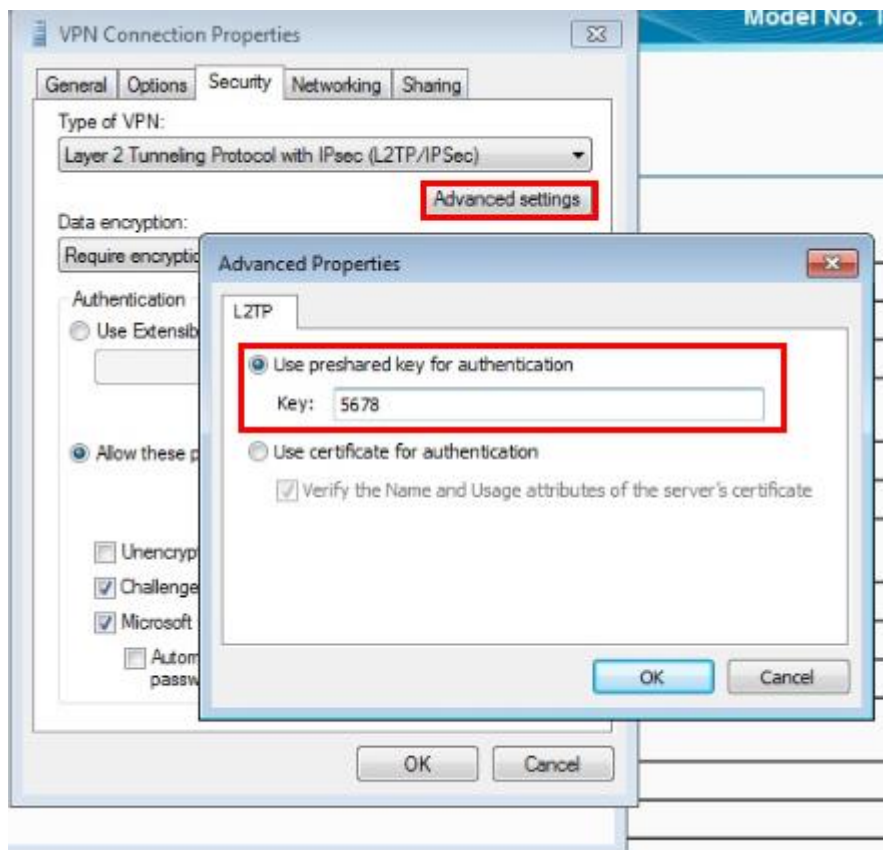
Step 9:

Right Click on VPN Connection and select Properties. On the Security tab, Select Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec), under Data encryption, select Require encryption (disconnect if server declines).



Step 10:

Click on Advanced settings, pick Use preshared key for authentication, and then enter the key, here is “5678”.



Step 11:

Double click on VPN Connection, enter User name and Password and then click on Connect.

