

# How to configure GreenBow IPsec VPN Client with a TP-Link VPN Router

## Configuring the TP-Link VPN Router

### Step 1:

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

The screenshot shows the router's configuration page with several sections:

- 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 is Link Up with Primary Connection: PPPoE/Russian PPPoE, Status: Connected, IP Address: 183.14.247.247 (highlighted in red), Subnet Mask: 255.255.255.255. WAN2 is Link Down with Primary Connection: Dynamic IP, Status: Connecting... IP Address: 0.0.0.0, Subnet Mask: 0.0.0.0. Annotations: A green box points to WAN1 IP with text "This IP address should be typed in GreenBow software as remote gateway." Another green box points to WAN1 Subnet Mask with text "This is Remote LAN subnet address for GreenBow software".
- LAN/DMZ:** Interface: LAN, IP Address: 192.168.0.1 (highlighted in red), Subnet Mask: 255.255.255.0 (highlighted in red), DHCP Server: Enabled, MAC Address: 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.

The screenshot shows the IKE Proposal configuration page:

- IKE Proposal:** Proposal Name: 1; Authentication: MD5; Encryption: 3DES; DH Group: DH2. Buttons: Save, Clear, Help.
- List of IKE Proposal:** Table with columns: No., Name, Auth, Encr, DH, Action. Row 1: No. 1, Name 1, Auth MD5, Encr 3DES, DH DH2, Action (edit/delete icons).

**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"/>	<input type="button" value="Save"/> <input type="button" value="Clear"/> <input type="button" value="Help"/>
Exchange Mode:	<input checked="" type="radio"/> Main <input type="radio"/> Aggressive	
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 (1-600)	
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, 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:	<input type="text" value="123"/>	<input type="button" value="Save"/> <input type="button" value="Clear"/> <input type="button" value="Help"/>
Security Protocol:	<input type="text" value="ESP"/>	
ESP Authentication:	<input type="text" value="MD5"/>	
ESP Encryption:	<input type="text" value="3DES"/>	

**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 Save

**IPsec Policy**

Policy Name: 123

Mode: Client-to-LAN Select Client-to-LAN

Local Subnet: 192.168.0.0 / 24

Remote Subnet: 0.0.0.0 / 0

WAN: WAN1

Remote Host: 0.0.0.0

Policy Mode:  IKE  Manual

IKE Policy: 123

IPsec Proposal 1: 123

IPsec Proposal 2: ----

IPsec Proposal 3: ----

IPsec Proposal 4: ----

PFS: NONE

SA Lifetime: 28800 Sec (120-604800)

Status:  Activate  Inactivate

Save  
Clear  
Help

**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**.

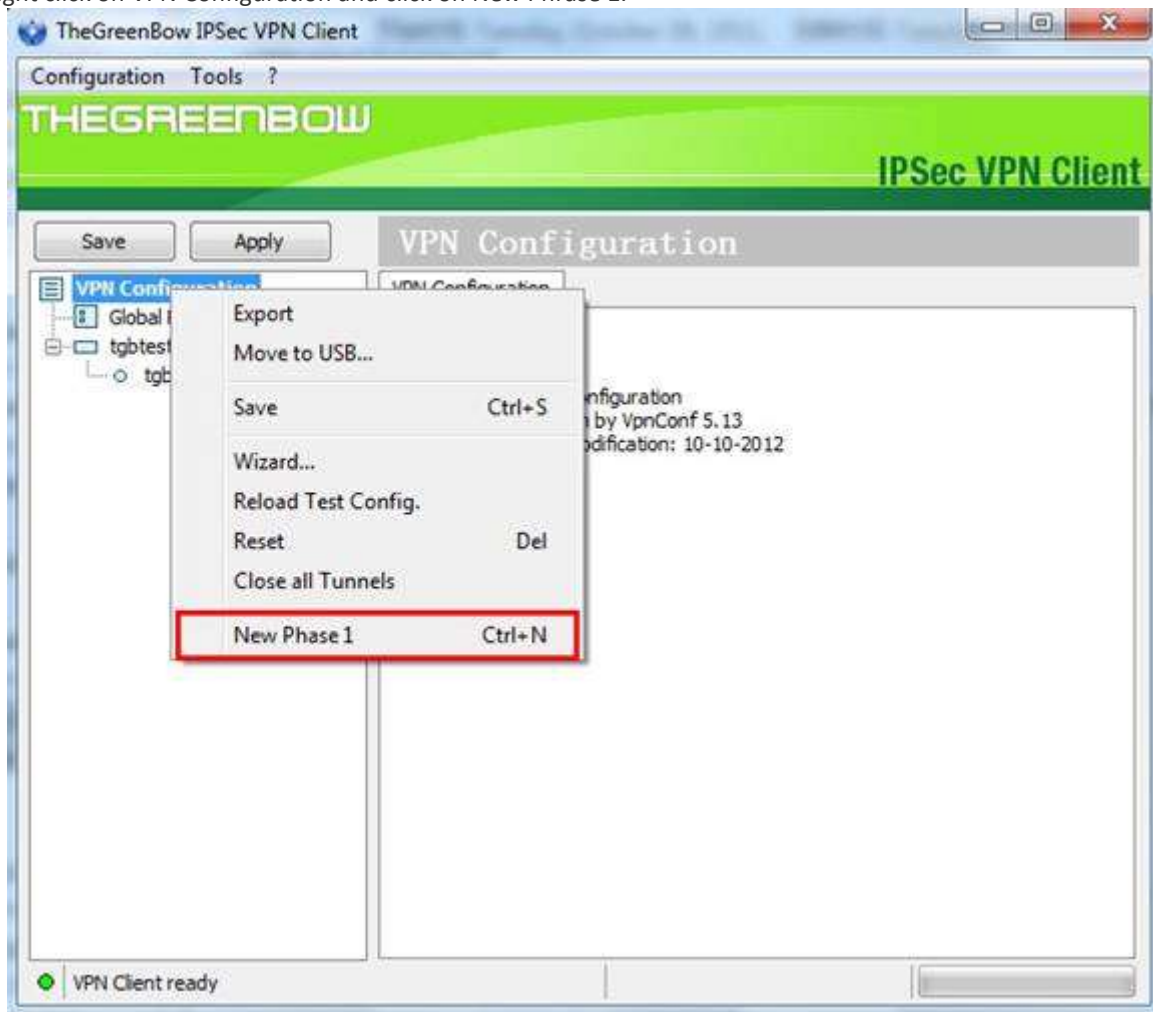
**Step 9:**

Enable **IPsec** and then click on **Save**.

## Configuring the GreenBow VPN Client

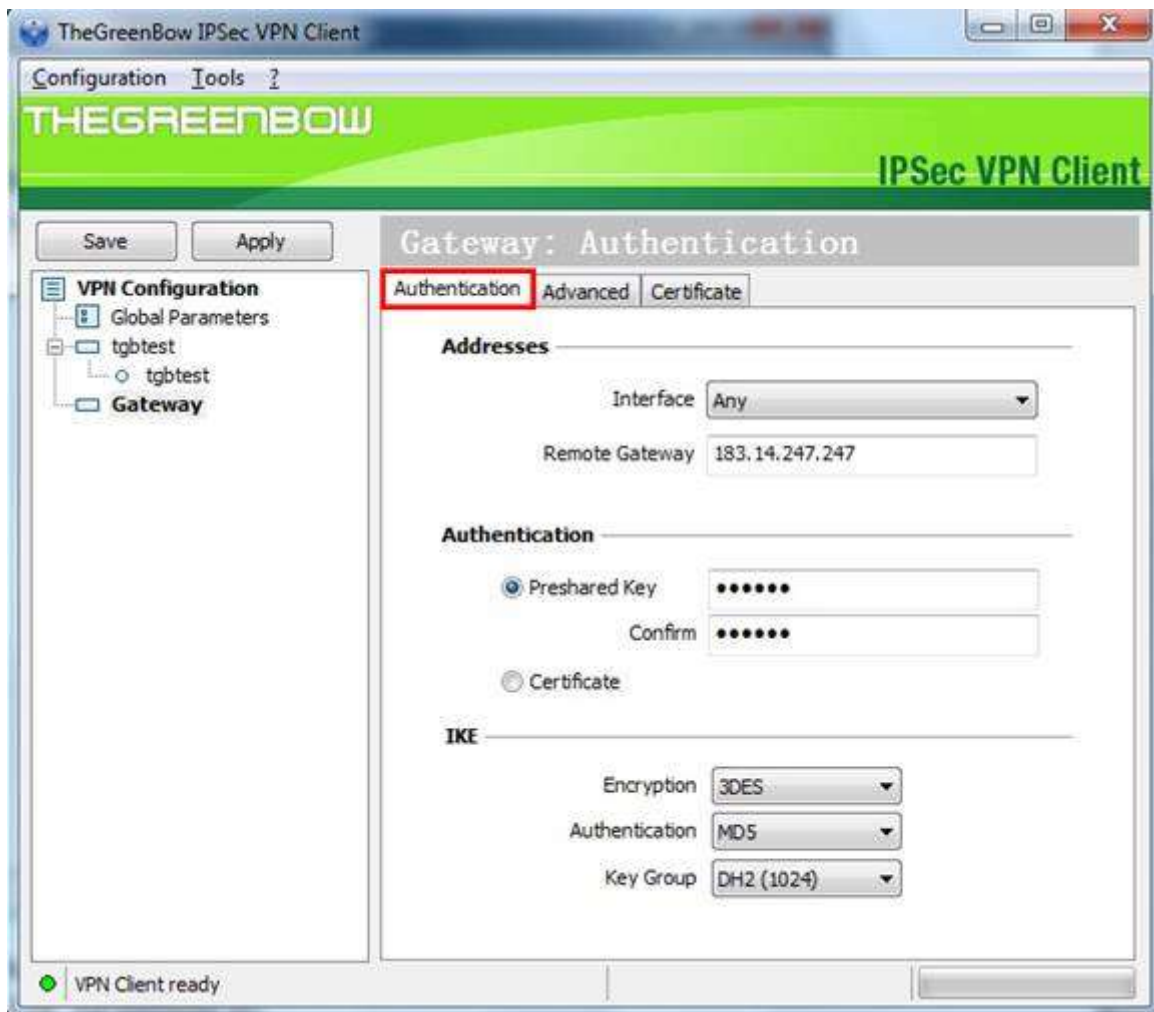
### Step 1:

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



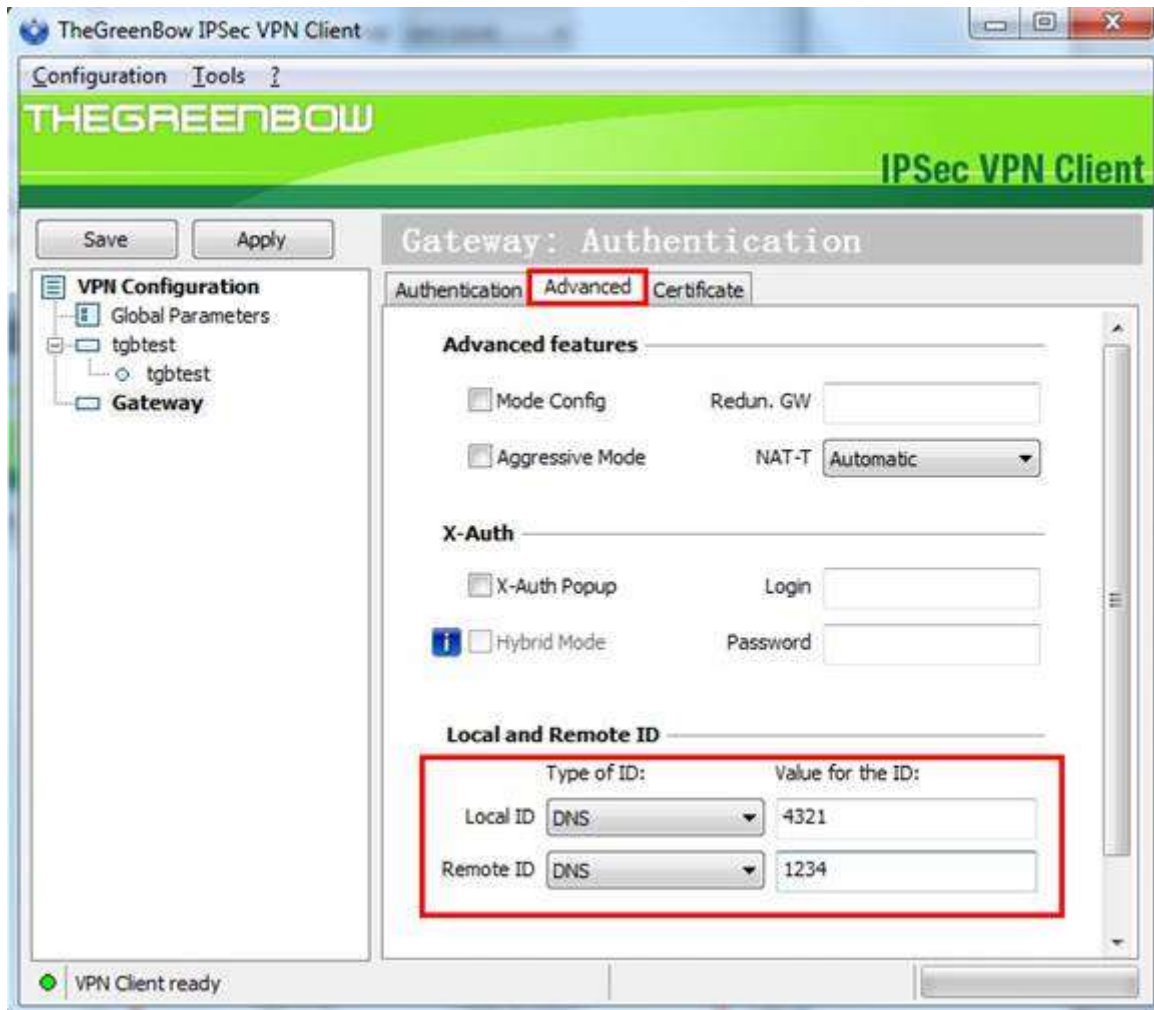
### Step 2:

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**, **MD5** and **DH2** here.

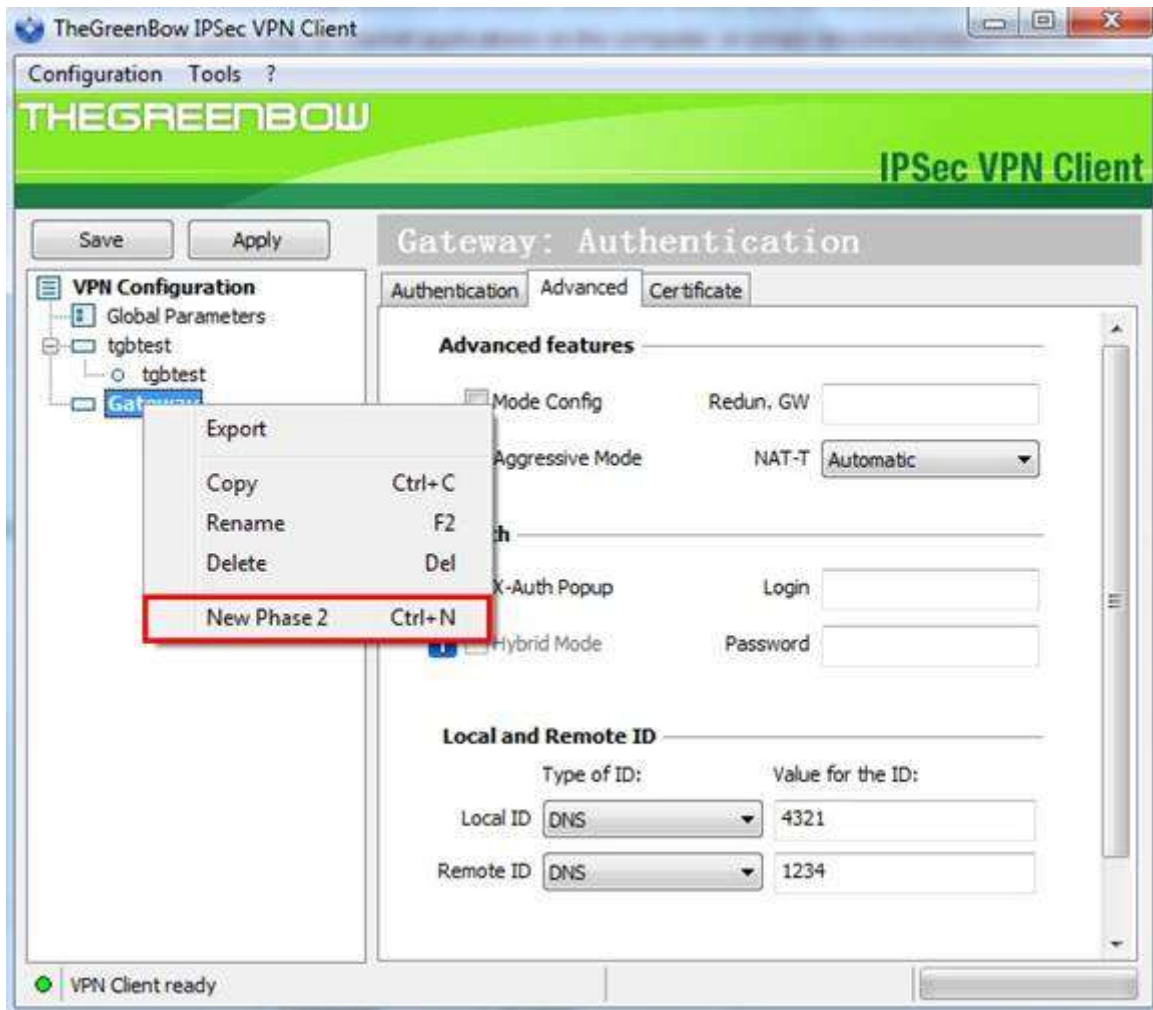


**Step 3:**

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

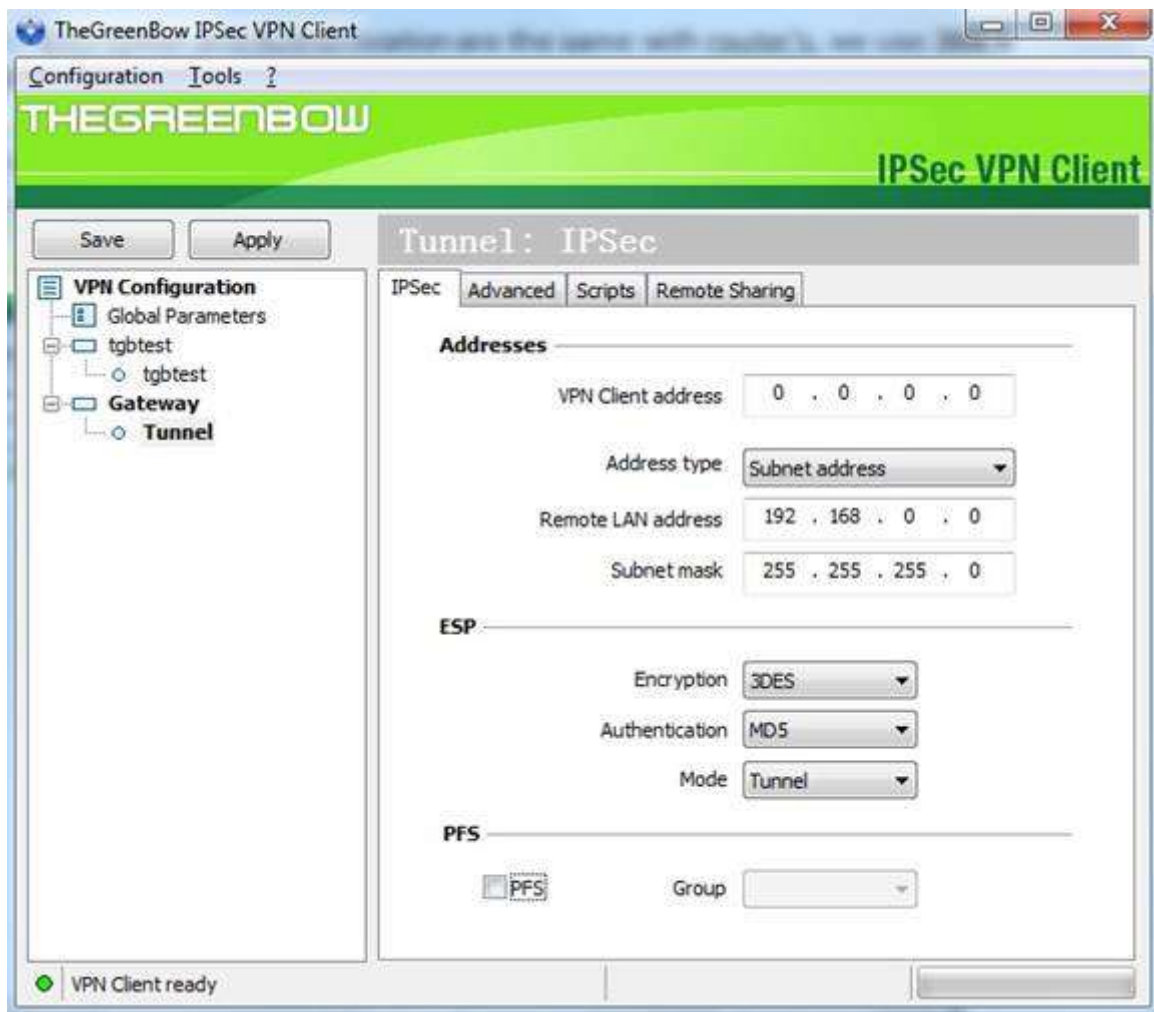


**Step 4:**  
Right click on Phase 1, add a new phrase 2.



**Step 5:**

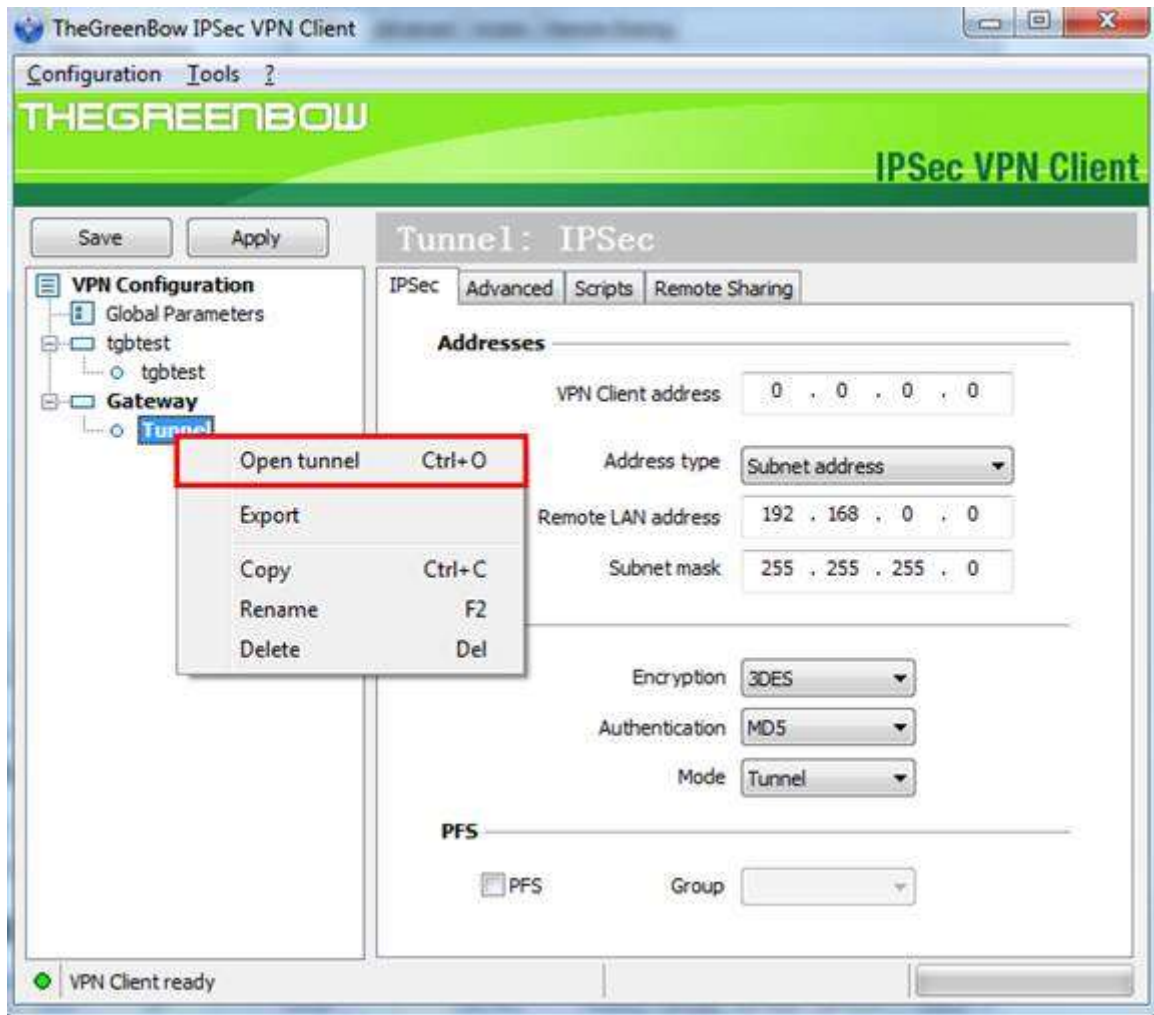
Enter remote LAN address and Subnet mask, in the example, the IP address is 192.168.0.0, Subnet mask is 255.255.255.0. Encryption and Authentication are the same with routers; we use **3DES** and **MD5** here. The Mode should be **Tunnel**.



**Step 6:**

Save the configuration and 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