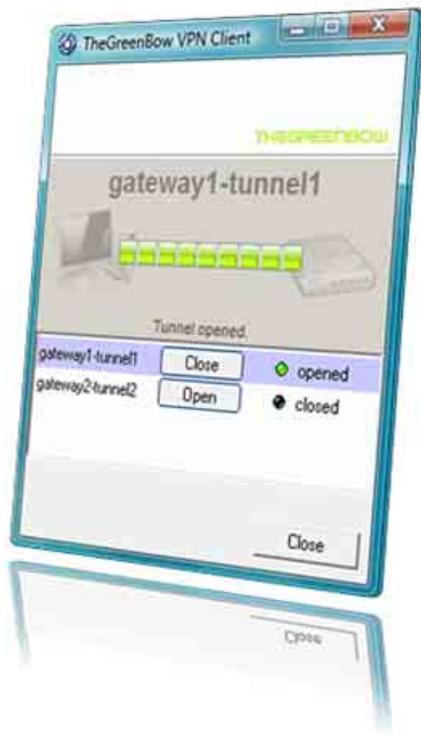


TheGreenBow™ IPsec VPN Client

Creating an IPsec Tunnel to a DR-250



Contents

Introduction.....	Page 3
Section 1 - DR-250 VPN Configuration.....	Page 4-5
Section 2 - TheGreenBow™ VPN Client Configuration.....	Page 6-9

Technical Support

If you require assistance with any of the instructions in this application note you can contact Westermo as follows:

Web:	www.westermo.co.uk
Technical e-mail:	technical@westermo.co.uk
Telephone:	+44 (0)1489 580585
Fax:	+44 (0)1489 580586

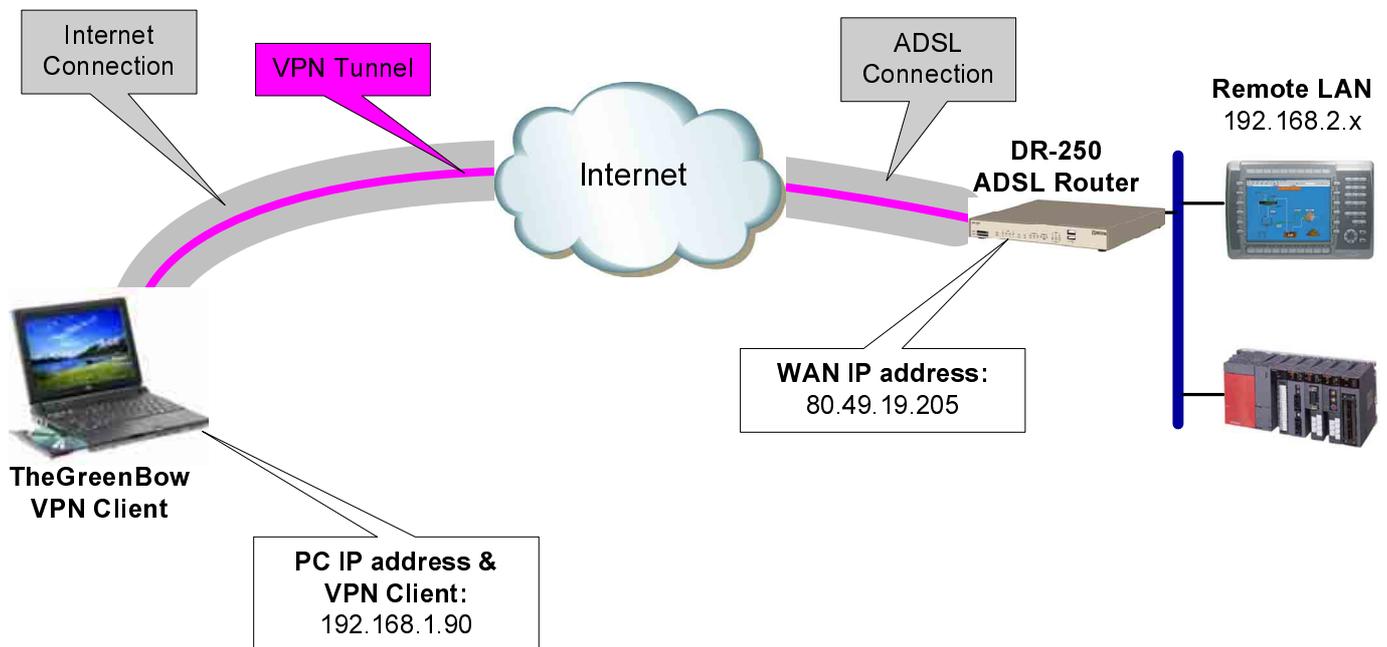
1. Introduction

This application note explains how to configure TheGreenBow™ VPN IPsec client to create a VPN tunnel to a Westermo DR-250 router. TheGreenBow™ VPN IPsec client is a commercially licensed software program and a 30 day evaluation version is available at www.thegreenbow.com.

This program has been chosen to complement the DR series of routers as it provides an easy to use desktop VPN client. Westermo recommend that the TheGreenBow™ client is used in all applications where access is required from a computer to a remote LAN. For LAN to LAN applications using routers refer to the Westermo VPN application note.

This application note was tested with version 4.20.006 of the TheGreenBow™ client.

The drawing below gives an overview of how the connections work. The IP addresses shown below relate to those used for the settings on the following pages. This will make it easier to understand what each setting is for. The desktop PC could be part of a company network or a stand alone PC, the only criteria is that it has access to an internet connection, and any firewall in use must be configured to allow IPsec Tunnels.



Section 1 - DR-250 VPN Configuration

This application note assumes the DR-250 has already had the ISP credentials entered the WAN interface and that the ADSL line has a public, static IP address.

The DR-250 needs to be configured to accept an incoming VPN from TheGreenBow™ client. Follow the numbered steps to complete this configuration.

The screenshot shows the 'Configure: IKE 0 (Initiator)' page. The left sidebar contains a navigation menu with 'VPN Configuration' expanded to show 'IKE Initiator' selected. The main content area contains various configuration fields for the IKE initiator. Three red arrows point from callout boxes to specific elements: the first points to the 'IKE Initiator' link in the sidebar, the second points to the 'Aggressive mode' dropdown set to 'On', and the third points to the 'OK' button at the bottom of the configuration form.

Logon to the DR-250 and click on the "VPN Configuration" followed by "IKE Initiator"	1
Switch Aggressive to "On"	2
Now click on the "OK" button to keep the settings	3

Section 1 - DR-250 VPN Configuration

Configure: IPsec EROUTE 0

To create a new VPN tunnel select an available IPSEC Eroute and fill in the parameters as shown **4**

Peer ID: ID of VPN Client **5**

Our ID: ID for Eroute 0 from this router **5**

Local subnet address: Set IP subnet address for local port & mask as shown **6**

Remote subnet address: Set IP address of remote VPN client & mask as shown **6**

Mode: Set to "Tunnel" **8**

AH authentication: Set to "Off" **8**

ESP authentication: Set to "MD5" **8**

ESP encryption: Set to "3DES" **8**

Duration (s): Set to "28800" **9**

Duration (kb): Set to "0" **9**

No SA action: Set to "Drop Packet" **9**

Create SA's automatically: Set to "No" **9**

Authent' method: Set to "Preshared Keys" **9**

Now click on the "OK" button to keep the settings **10**

Click on "Users" and select a free user to create the Preshared Key. It is good practice to create the PSK at User 10, or above, to prevent conflicts with the router logons. **11**

Configure: User 15

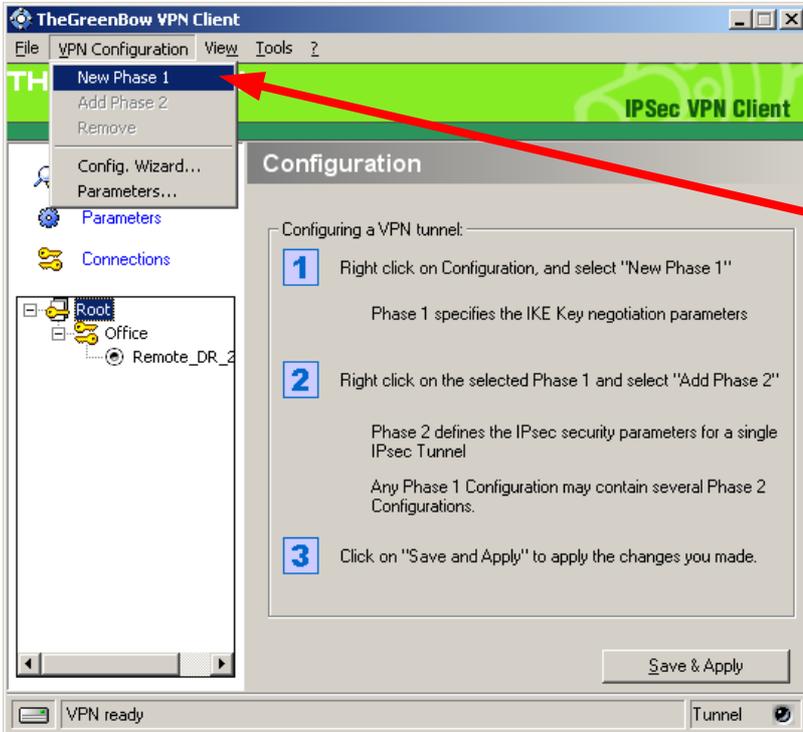
Name: This must be the same as the "Peer ID" entered in the Eroute **12**

Password: This is the entry for the preshared Key and must be the same as the PSK entered for the VPN client **12**

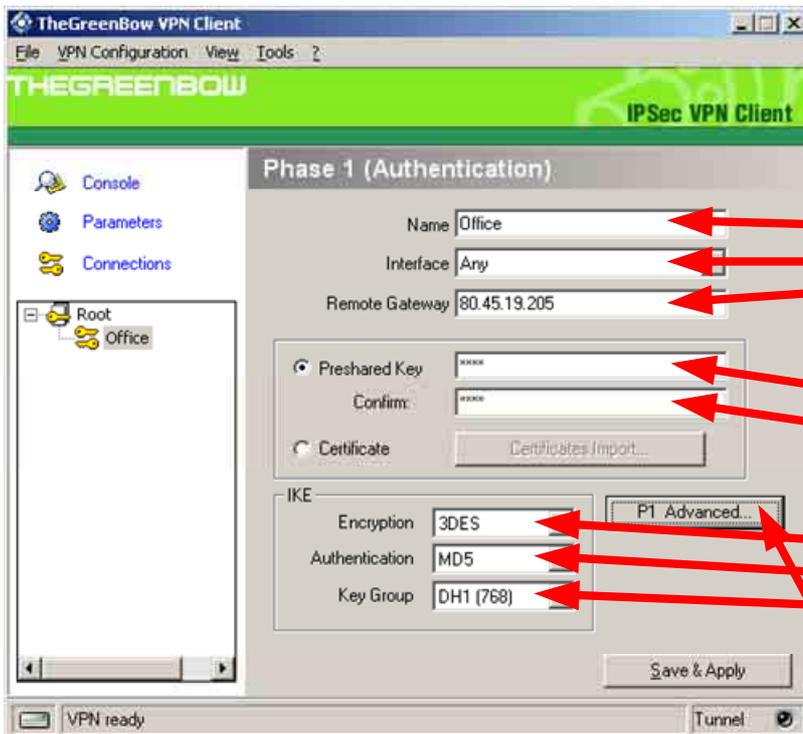
Now click on the "OK" button to keep the settings. Finally, click on the "save to flash" link and select hit the "OK" button to store the configuration in the router's memory. **13**

Section 2 - TheGreenBow™ VPN Client Configuration

Now follow the numbered steps to configure TheGreenBow™ VPN client to connect to the Eroute configured within the DR-250.



<p>To create a new VPN tunnel go to “VPN Configuration” and select “New Phase 1”</p>	1
--	---



<p>Name: Text label for this location Interface: Set to “Any” or IP address of PC Remote Gateway: Enter the IP address of the remote router (WAN port)</p>	2
---	---

<p>Preshared Key: The key must be the same word/number as the password/PSK configured in the DR-250 router for this VPN</p>	3
--	---

<p>Encryption: Set to “3DES” Authentication: Set to “MD5” Key Group: Set to “DH1 (768)”</p>	4
--	---

<p>Now click on the “P1 Advanced” button to configure the IPsec parameters</p>	5
--	---

Section 2 - TheGreenBow™ VPN Client Configuration

Phase1 Advanced

Advanced features

Config Mode Redund.GW:

Aggressive Mode NAT-T: **Automatic**

X-Auth

X-Auth Popup Login:

Hybrid Mode Password:

Local and Remote ID

Choose the type of ID: Set the value for the ID:

Local ID: **KEY ID**

Remote ID: **KEY ID**

Aggressive Mode: Enable this option
NAT-T: Set to **"Automatic"**

6

Local ID: Set to **"KEY ID"** and set the value to match the **"Peer ID"** set in the DR-250
Remote ID: Set to **"KEY ID"** and set the value to match the **"Our ID"** set in the DR-250

7

Now click on the **"OK"** button to store the Phase 1 Advanced settings

8

TheGreenBow VPN Client

File VPN Configuration View Tools ?

THEGREENBOW IPsec VPN Client

Phase 1 (Authentication)

Name:

Interface:

Remote Gateway:

Preshared Key Confirm:

Certificate

IKE

Encryption:

Authentication:

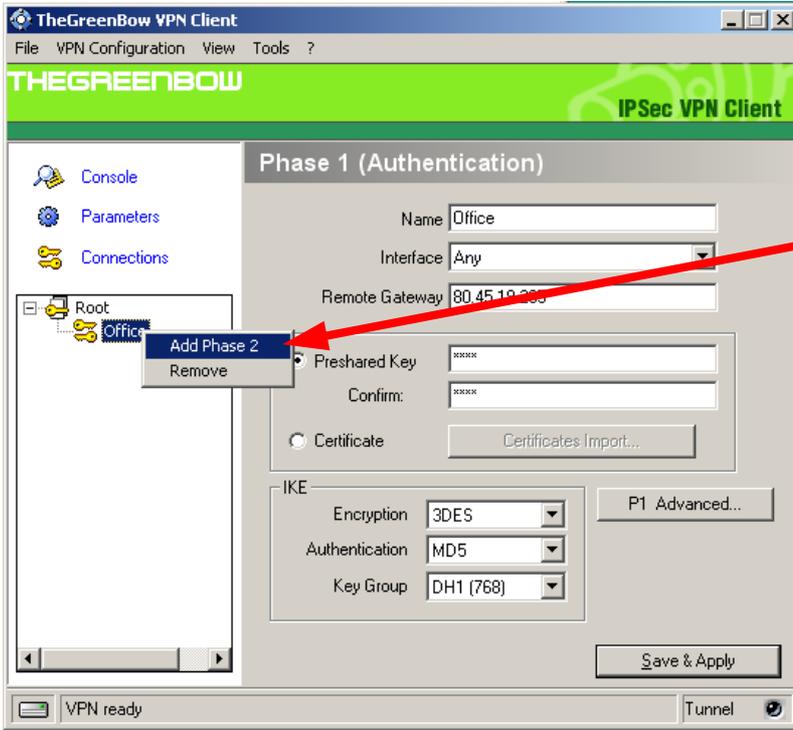
Key Group:

VPN ready Tunnel

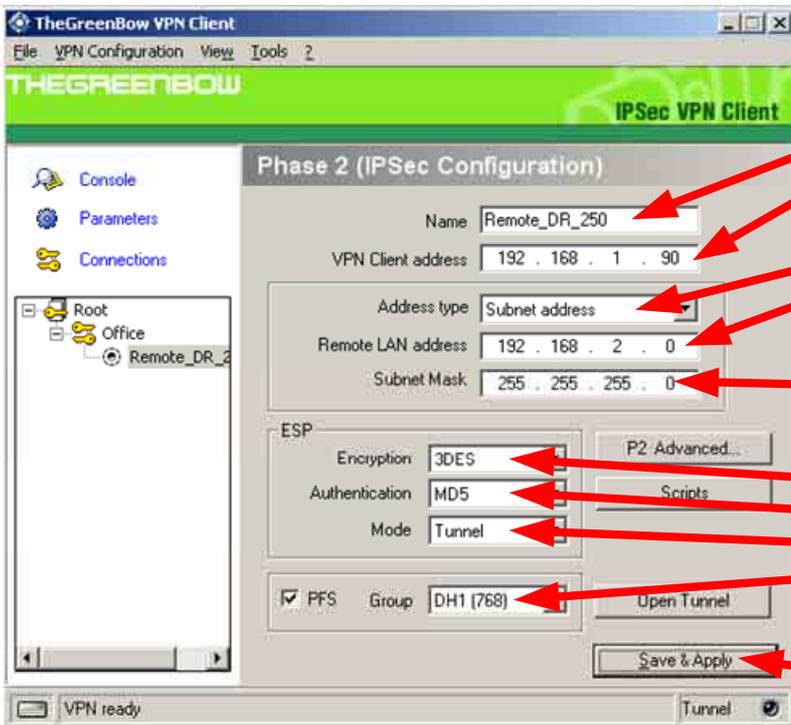
Now click on the **"Save & Apply"** button to store the Phase 1 VPN settings

9

Section 2 - TheGreenBow™ VPN Client Configuration



Right click on the new VPN and select the **"Add Phase 2"** option 10



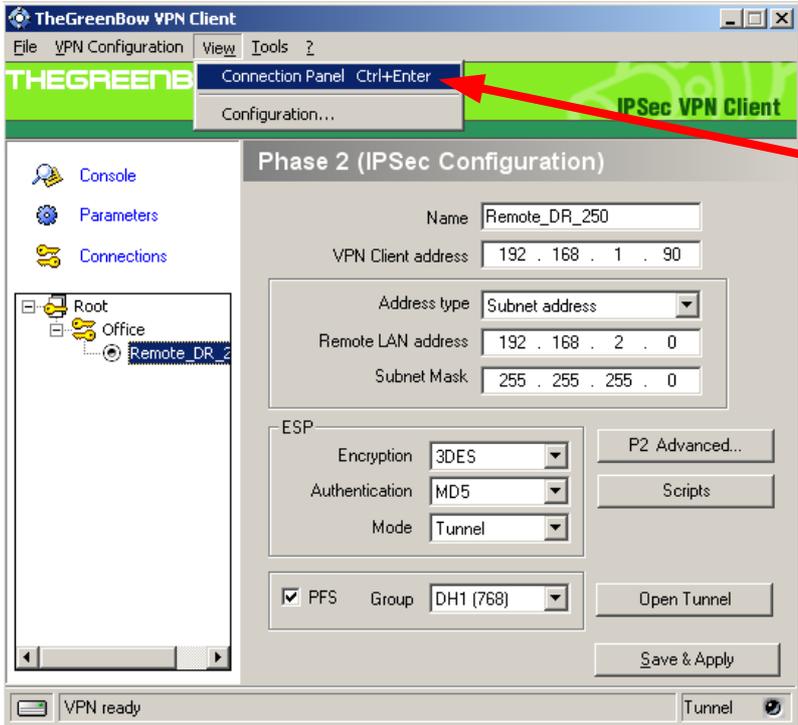
Name: Text label for the remote location
VPN Client Address: This must be the same as the **"Remote subnet address"** in the DR-250 Eroute 11

Address type: Set to **"Subnet address"**
Remote LAN address: This must be the same as the **"Local subnet address"** in the DR-250 Eroute
Subnet mask: This must be the same as the mask in the DR-250 Eroute 12

Encryption: Set to **"3DES"**
Authentication: Set to **"MD5"**
Mode: Set to **"Tunnel"**
Group: Enable PFS and select **"DH1 (768)"** 13

Now click on the **"Save & Apply"** button to save the Phase 2 parameters 14

Section 2 - TheGreenBow™ VPN Client Configuration



Go to the "View" option on the menu and select "Connection Panel" 15



To open the VPN tunnel, click on this button 16



If all of the settings are correct, the tunnel will open and the status will be as shown. At this point the remote LAN is now accessible. 17

Notes