

D-Link And TheGreenBow Solution

DFL-800 Netdefend IPS/UTM Firewall Application Note

Version 2.01
(2009-10-24)



Revision History

Date	Rev.	Description	Editor
2009-4-24	1.0	Interoperability Compliance Testing Negotiate mode for Phase1 and Phase2 using TheGreenBow VPN Client software and D-Link product's DFL-800.	John Yoong
2009-5-28	2.0	Added the function VPN User Authentication using TheGreenBow VPN Client software (X-Auth) and DFL- 800 (External Radius Server) and changed the network diagram.	John Yoong
2009 -10-24	2.01	Changing DFL-800 firmware from 2.20.00 to 2.26.00.06 and TheGreenBow VPN Client firmware 4.60.00 to 4.61.003 and edit TheGreenBow client picture for "PFS" setting.	John Yoong

1. Introduction

The objective of this document is to provide a guide describing how to configure the devices to achieve the same environment as show at the network topology.

Users of this document are expected to already possess basic knowledge of D-Link devices and TheGreenBow VPN software, and are familiar with how to perform basic configurations. Only important configurations, such as those pertaining to interfacing and integrating, will be described in this document.

For purpose of reference, configuration files for each device are available for download.

2. Audience

This document is intended for project engineers or end users that need to implement DFL series and TheGreenBow software at the sites.

3. Objective

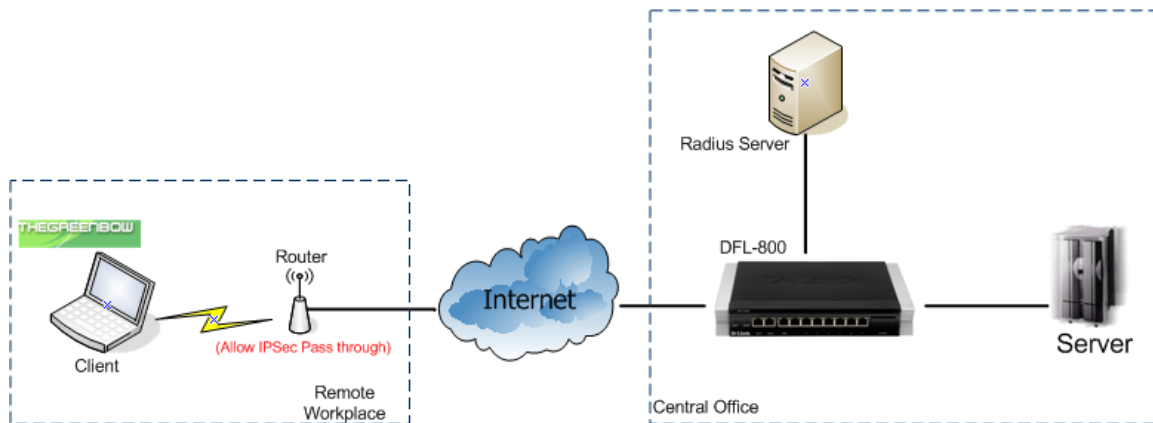
This topology consist the scenarios that integrates using TheGreenBow VPN program and D-Link Firewall and demonstrate integrations and network solutions to OBUs, and in addition, to Partners and Customers from D-Link International.

4. List of Equipment and Software

The table below shows the devices information.

Device No.	Device Name	Device Model	Firmware
1	TheGreenBow VPN Client Software	-	4.61.003
2	Netdefend IPS Firewall	DFL-800	2.26.00.06-12649
3	WinRadius Radius Server	-	4.00

5. Network Diagram



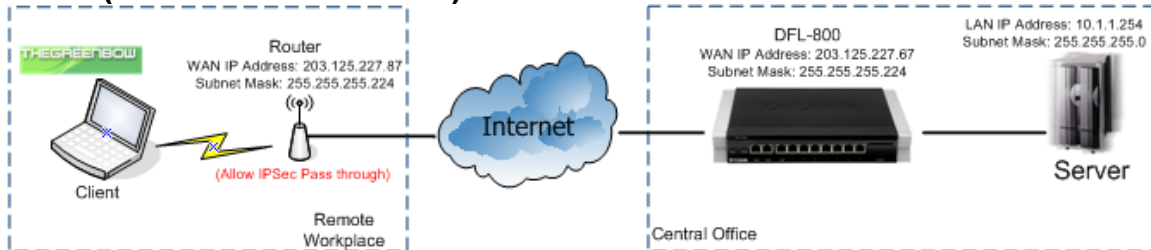
Note: Router is set to allow IPSec pass through.

6. Configurations

In this document, we will only describe the main configurations for this Scenario. The configurations setting for all the D-Link products will not be described here and for more detail about the product you can download their user guide.

- 1) **TheGreenBow VPN Client (IPSec) and D-Link Security Solutions (VPN Client → DFL-800)**
- 2) **TheGreenBow VPN Client (XAuth) and D-Link Security Solutions (VPN Client → DFL-800 → Radius Server)**

6.1 TheGreenBow VPN Client (IPSec) and D-Link Security Solutions (VPN Client → DFL-800)



In this scenario the user can connect back to the headquarter database by using TheGreenBow VPN Client connection to DFL-800.

All configurations are based on DFL-800 (F/W: **2.26.00.06-12649**) and TheGreenBow VPN Client (F/W: **4.61.003**)

The steps in this configuration are:

- **Setup DFL-800 for VPN tunneling**
 - Setup Pre-shared Key
 - Phase 1 and Phase 2 algorithms setup
 - Setting up IPSec-Tunnel
 - Setup IP Rules
- **Setup TheGreenBow VPN Client software**
 - Setup Phase 1
 - Setup Phase 2

6.1.1) Setup DFL-800 for VPN tunneling

6.1.1.1) Setup Pre-Shared Key

- 1) Login to the DFL-800 and click **“Authenticate Objects”** and add a new **“Pre-shared Key”** and fill in the passphrase and name.

D-Link
Building Networks for People

Logged in as administrator
admin - 2013/12/22 10:17

Home Configuration Tools Status Maintenance Logout Help

IPSec-Pre-Shared-Key_1
PSK(Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

General

Name:

Shared Secret

Passphrase

Shared Secret:

Custom Secret:

☐ Hexadecimal Key

Passphrase:

Since regular words and phrases are vulnerable to dictionary attacks, do not use them as shared secrets.

6.1.1.2) Phase 1 and Phase 2 algorithms setup

- 1) At the **“IKE Algorithms”**, select the Encryption and Integrity algorithms for your phase 1 authenticate.

D-Link
Building Networks for People

Logged in as administrator
admin - 2013/12/22 10:17

Home Configuration Tools Status Maintenance Logout Help

PH1_3DES-SHA1
Configure algorithms which are used in the IKE phase of an IPSec session.

General

Name:

Encryption Algorithms

	Preferred	Min	Max
<input type="checkbox"/> Null			
<input checked="" type="checkbox"/> DES	64	64	64
<input checked="" type="checkbox"/> 3DES	192	192	192
<input type="checkbox"/> CAST128	128	128	128
<input type="checkbox"/> Blowfish	128	128	448
<input type="checkbox"/> Twofish	128	128	256
<input checked="" type="checkbox"/> AES (Rijndael)	128	128	256

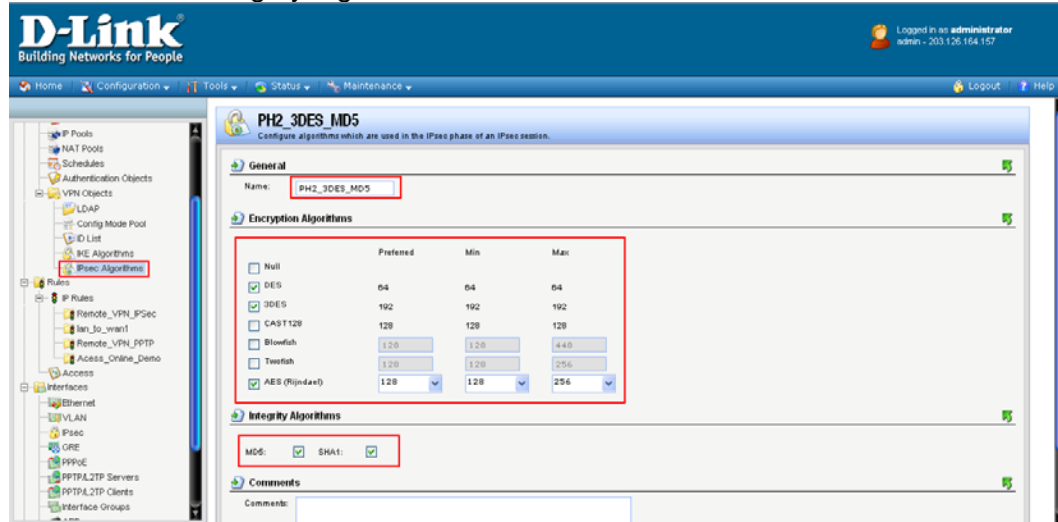
Integrity Algorithms

MD5: ☒ SHA1: ☒

Comments

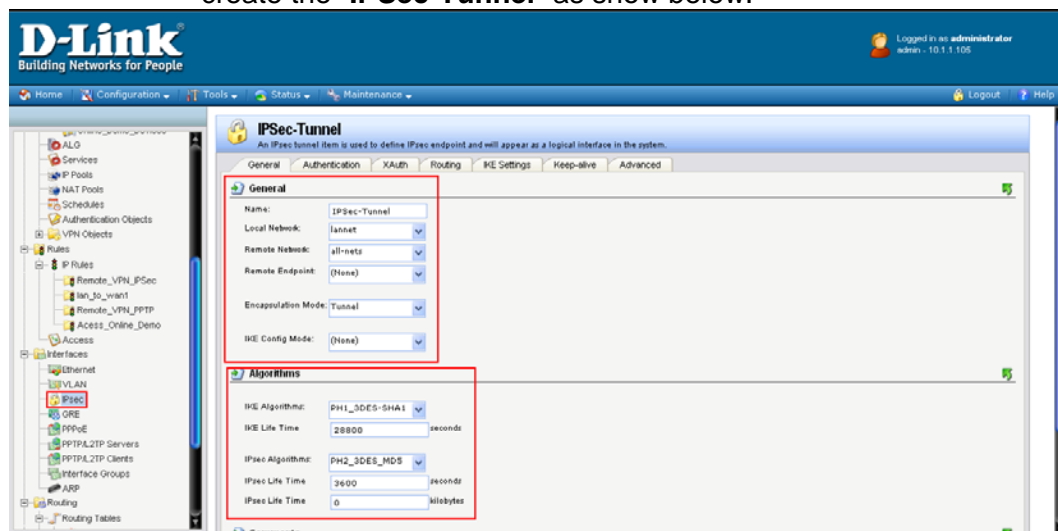
Comments:

- 2) Next is the “**IPSec Algorithms**”, select the Encryption and Integrity algorithms for the Phase 2.

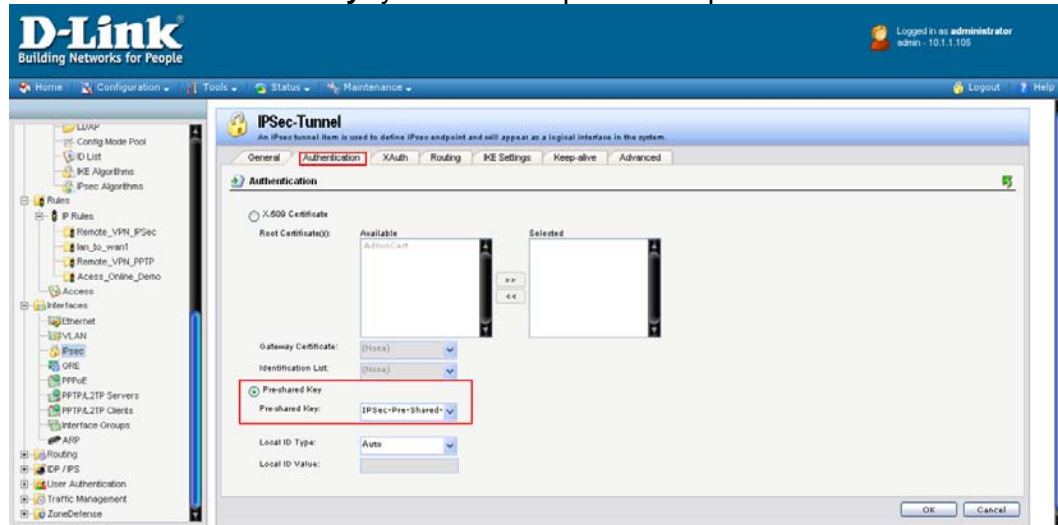


6.1.1.3) Setting up IPSec-Tunnel

- 1) After we finish setting up the algorithms, next we will need to create the “**IPSec-Tunnel**” as show below.



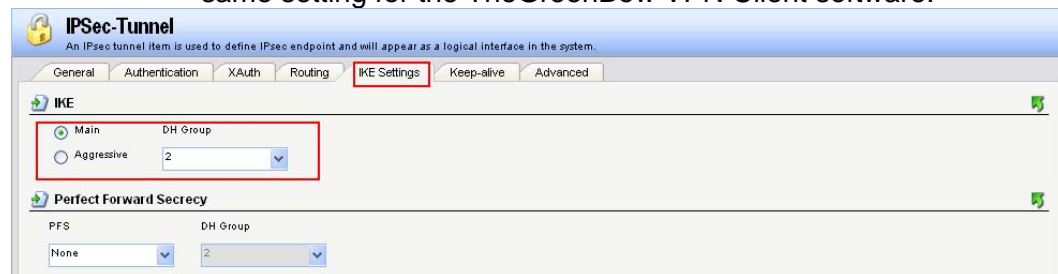
- 2) Next, click on the “**Authentication**” tab and select the “**Pre-Shared Key**” you have setup at the steps 1.



- 3) After selecting the Pre-Shared Key, next is to enable the “**Dynamically add route**” at the routing tab.



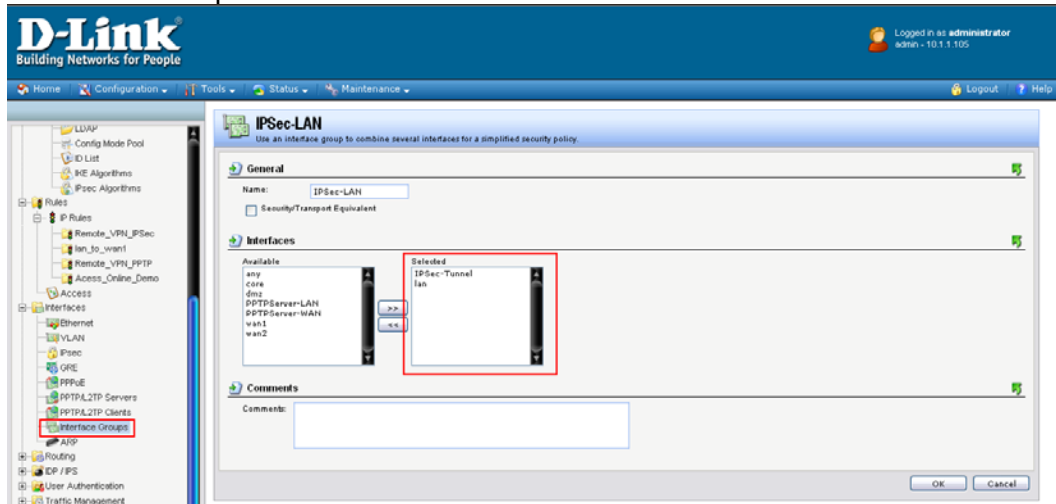
- 4) Last step is to make sure the DH Group at the IKE setting is the same setting for the TheGreenBow VPN Client software.



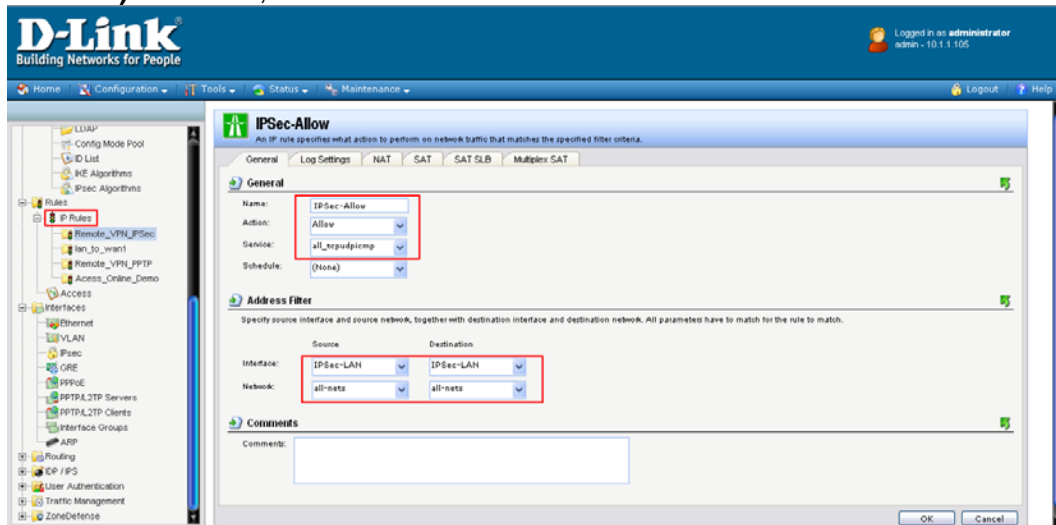
6.1.1.4) Setup IP Rules

Now is to setup the IP Rules so there the DFL-800 knows where to direct all the traffic to.

- 1) First add a new interface group name **"IPSec-LAN"** by grouping up **"IPSec-Tunnel"** and **"LAN"**.



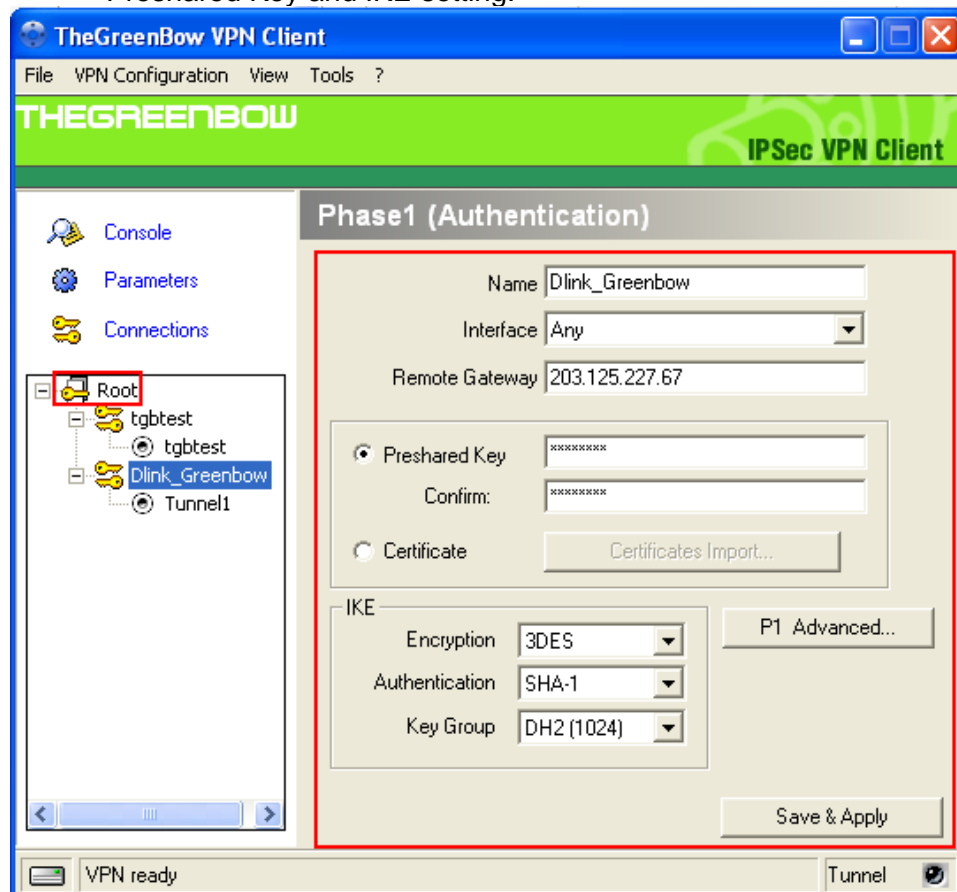
- 2) Next, click **"IP Rules"** and add a new IP rule as show below.



6.1.2) Setup TheGreenBow VPN Client Software

6.1.2.1) Setup Phase 1

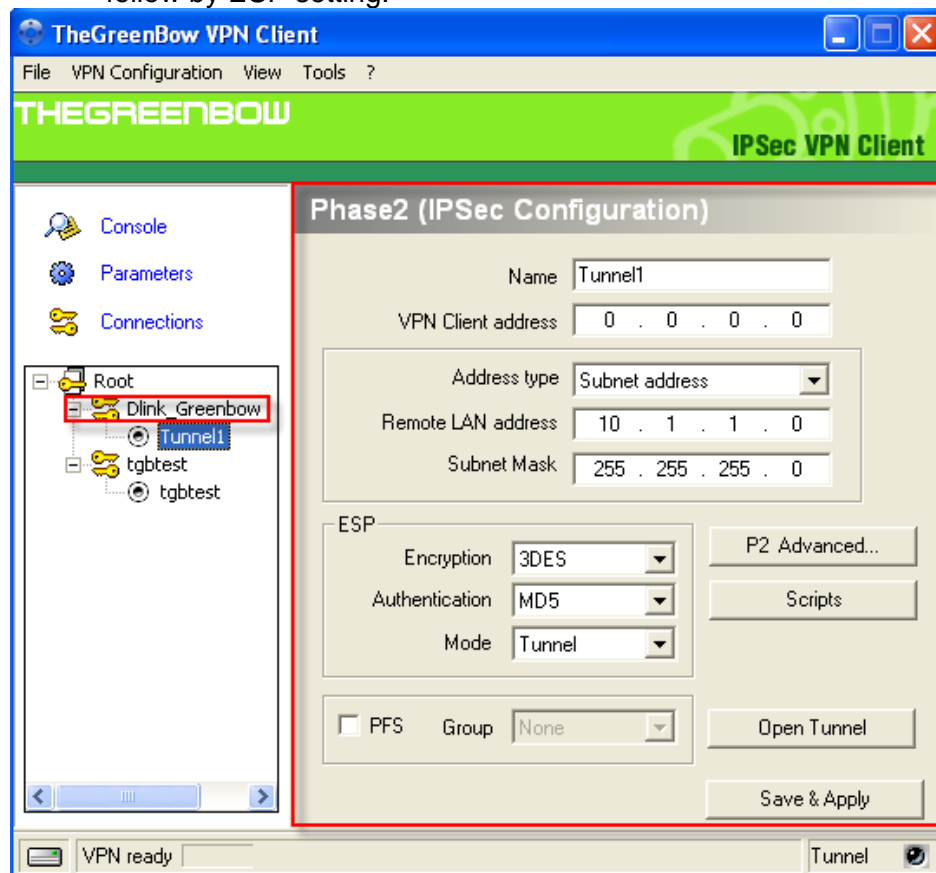
- 1) Right click on the “**Root**” to add a new “**Phase1**”, next fill in the IP address for this VPN client and Remote gateway IP follow by Preshared Key and IKE setting.



Note: the Preshared Key and IKE must be the same setting set in the DFL-800.

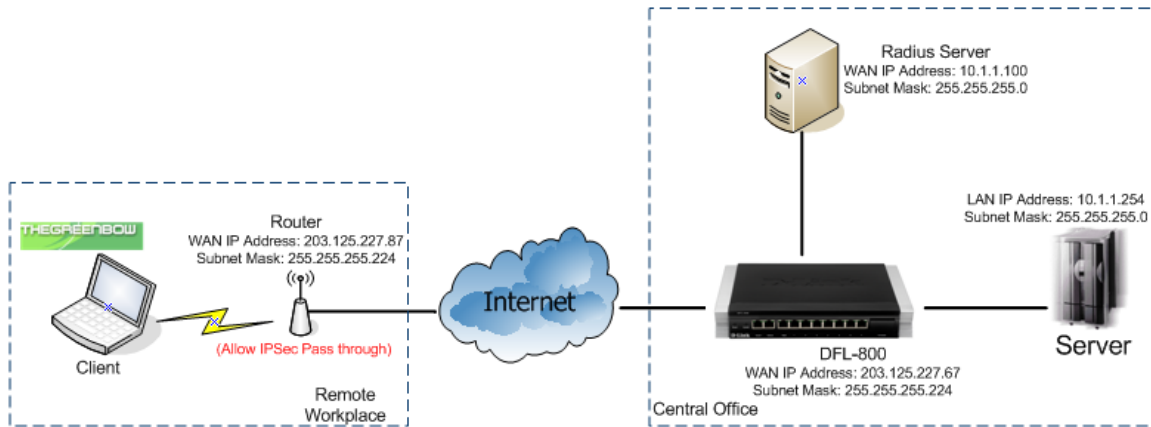
6.1.2.2) Setup Phase 2

- 1) Right click on the “**Phase1**” to add a new “**Phase2**”, next fill in the VPN Client address for this VPN client and Remote gateway IP follow by ESP setting.



Note: the ESP Encryption and Authentication setting must be the same in the DFL-800 IPSec-Tunnel.

6.2 TheGreenBow VPN Client Software (X-Auth) and D-Link security solutions (VPN Client→DFL-800)



In this scenario the client will be authenticate (X-Auth) before the user can connect back to the headquarter database by using TheGreenBow VPN Client connection to DFL-800 authenticate by External Authentication (Radius Server).

All configurations are based on DFL-800 (F/W: **2.26.00.06**), TheGreenBow VPN Client (F/W: **4.61.003**) and WinRadius (Version **4.00**)

*Note: Before configuration this solution, please make sure that your DFL-800 and VPN Client had the IPSec setting configured. Please refer to (6.1 - **TheGreenBow VPN Client software (IPSec)** and **D-Link Security Solutions (VPN Client → DFL-800)**)*

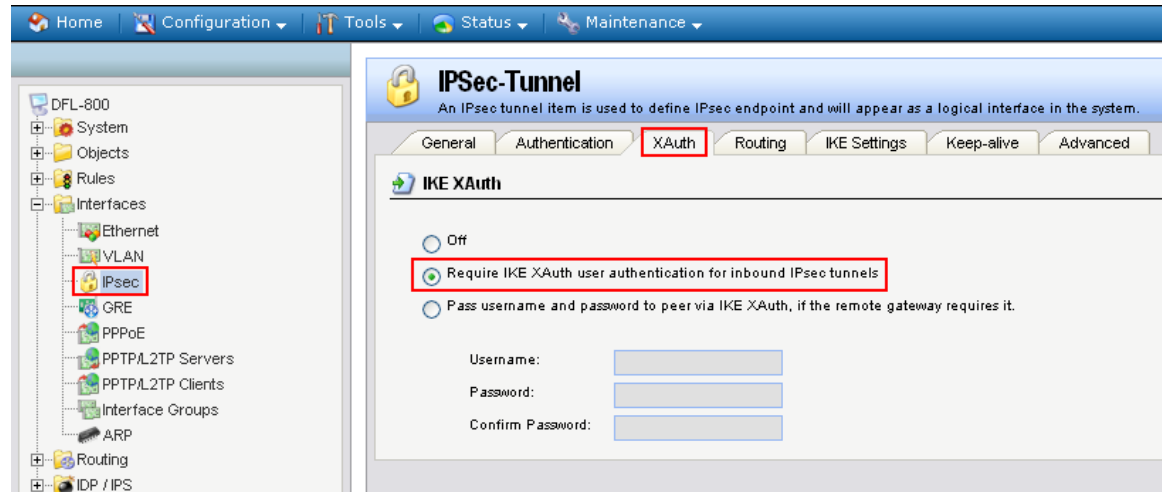
The steps in this configuration are:

- **Setup DFL-800 for X-Auth**
 - **Enable the X-Auth in DFL-800**
 - **Setup the External Authentication Server**
- **Setup TheGreenBow VPN Client software**
 - **Enable the X-Auth Function**
- **Setup WinRadius Server**
 - **Set the Secret Key**

6.2.1) Setup DFL-800 for X-Auth

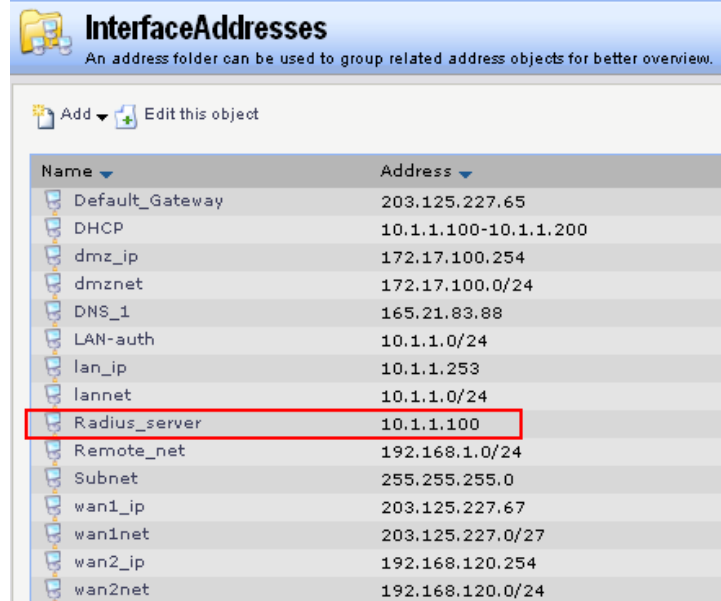
6.2.1.1) Enable the X-Auth in DFL-800

- 1) At the “**Interfaces → IPsec**”, select the IPsec tunnel you have created in the previous solution and at the “XAuth” tab, enable the function as show below.



6.2.1.2) Setup the External Authentication Server (i.e. Radius)

- 1) Add the IP Address for the Radius Server in the “**Address Book**”.



- 2) Select the “User Authentication → External User Database” and add a new “Radius Server” with the setting as show below.

The screenshot shows the D-Link web interface. On the left, the navigation tree is expanded to 'User Authentication' > 'External User Databases'. The main panel is titled 'Radius_server' and contains a 'General' tab. The configuration fields are as follows:

Field	Value
Name	Radius_server
IP Address	Radius_server
Port	1812
Retry Timeout	2 seconds
Shared Secret	*****
Confirm Secret	*****

Below the configuration fields is a 'Comments' section with a text area.

Note: the Shared Secret must be the same key in the Radius Server.

- 3) Next, add a New Rule in the “User Authentication Rules”.

The screenshot shows the D-Link web interface. On the left, the navigation tree is expanded to 'User Authentication' > 'User Authentication Rules'. The main panel is titled 'Xauth' and contains several tabs. The 'General' tab is active, showing the following configuration fields:

Field	Value
Name	Xauth
Agent	XAuth
Authentication Source	RADIUS
Interface	IPSec_lan
Originator IP	all-nets
Terminator IP	(None)

Below the configuration fields is a note: "For XAuth and PPP, this is the tunnel originator IP."

- 4) At the “**Authentication Options**”, select the Radius Server you have created and select the Radius Method as “**CHAP**”.

Xauth
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General Log Settings **Authentication Options** Accounting HTTP(s) Agent Options PPP Agent Options Restrictions

General
Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.

Radius Server(s):

Available	Selected
	Radius_server

Move up Move down

Radius Method: Challenge Handshak

Local User DB: Xauth

- 5) **Save and activate the setting.**

Save Configuration

Saving configuration, please wait..
The changes have been saved, and the unit is now activating the new configuration.

You must reconnect to it within 30 seconds for the configuration changes to be finalized. If this fails, the unit will revert to its previous configuration.

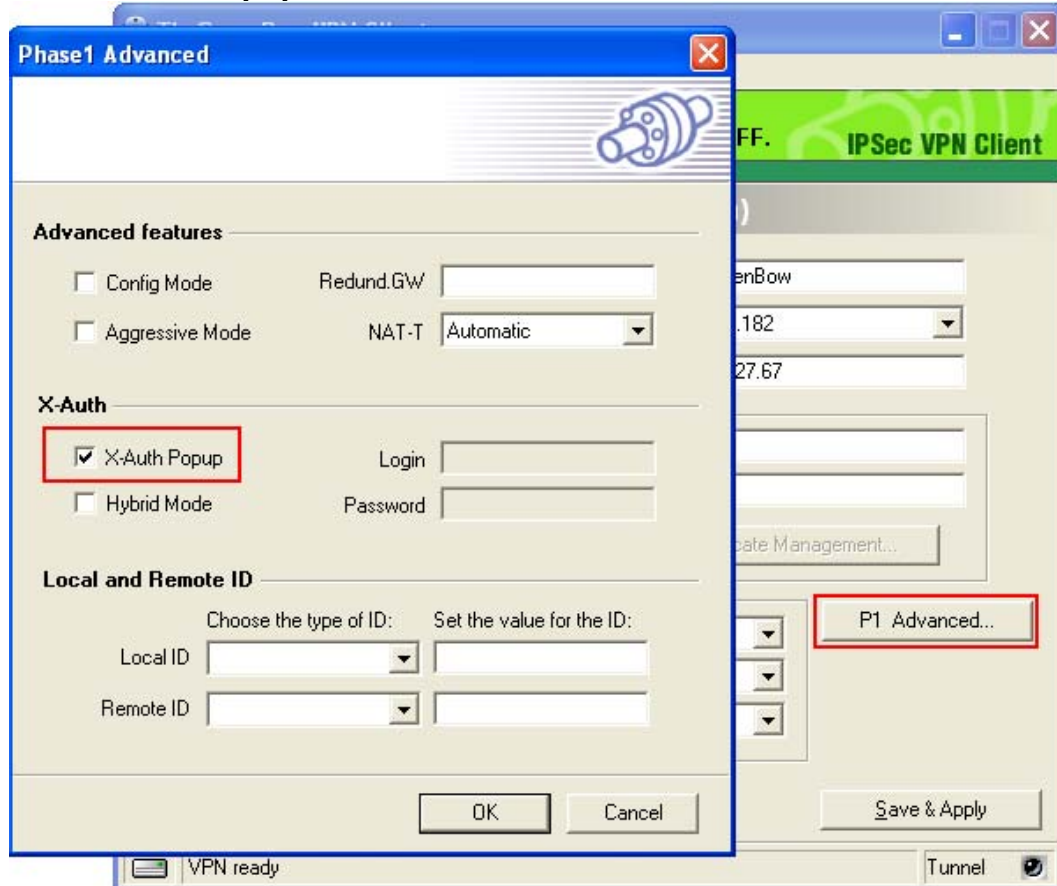
This page will automatically refresh in 24 seconds in an attempt to do this automatically.
If the automatic refresh fails, you can:

- Reconnect to the unit manually.
- Work out where to connect by yourself (necessary if interface IP address has changed)

6.2.2) Setup TheGreenBow VPN Client software

6.2.2.1) Enable the X-Auth Function

- 1) Inside the “**P1 Advanced**” menu, tick the box for the “**X-Auth Popup**”.

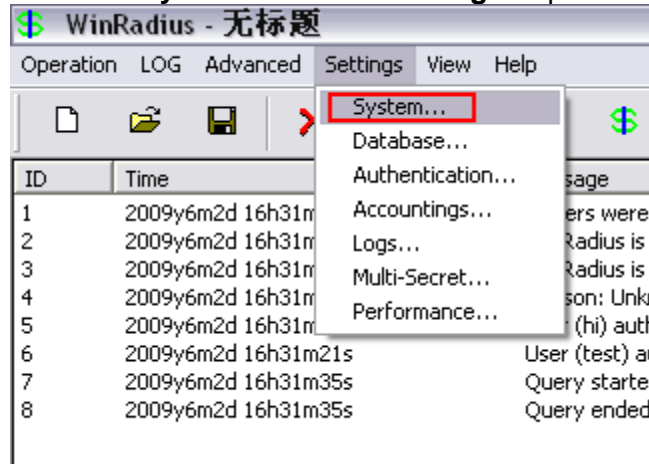


- 2) Click “**Ok**” and “**Save &Apply**” the setting.

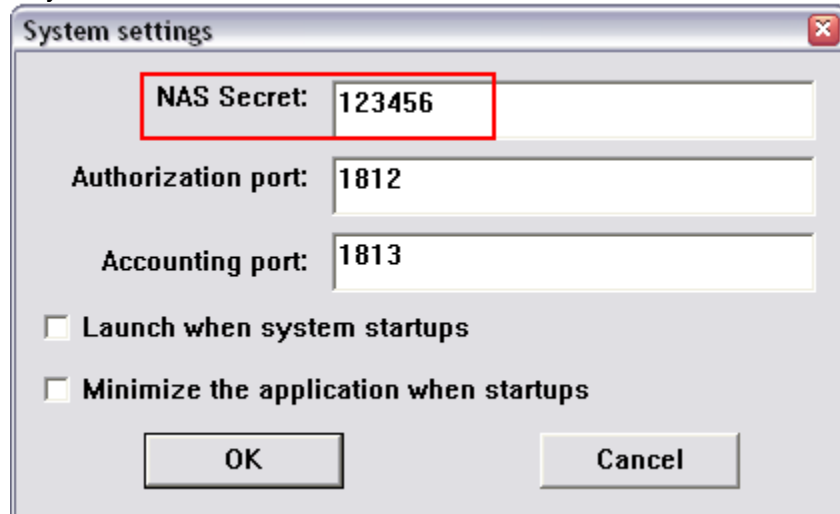
6.2.3) Setup WinRadius Server

6.2.3.1) Set the Secret Key

- 1) Click the “**System**” from the “**Setting**” drop down list



- 2) Key in the “**NAS Secret**”.



Note: The NAS Secret must be the same key set in the DFL-800 “Shared Key”.

- 3) Click “**OK**”, close and start the WinRadius Server again.

7. Interoperability Compliance Testing

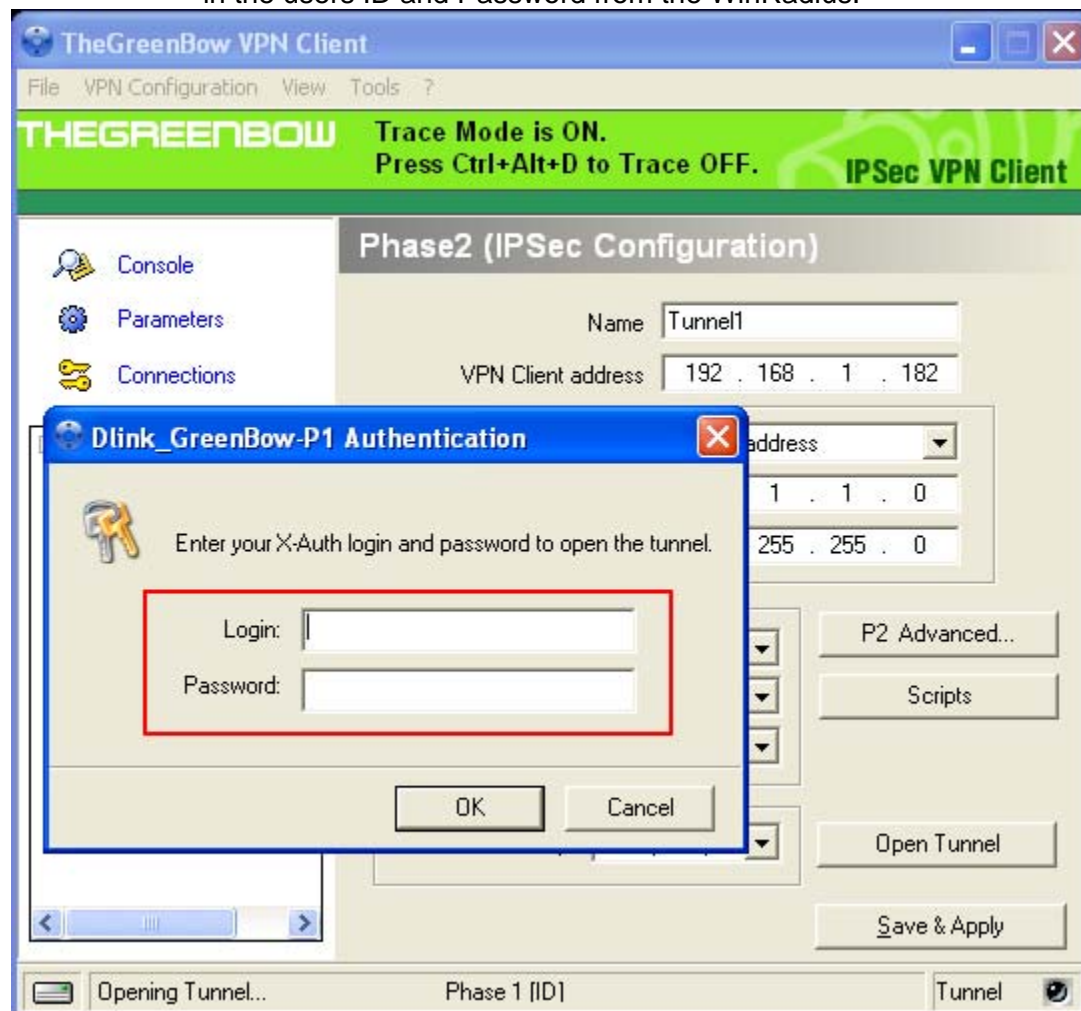
7.1) General Test Approach

- a. Open the VPN tunnel using different Negotiate Mode in phase 1 and phase 2:

Series Negotiate Mode	
Phase 1	Phase 2
AES-SHA	AES-SHA
AES-MD5	AES-SHA
3DES-MD5	AES-SHA
3DES-SHA	AES-SHA
DES-MD5	AES-SHA
DES-SHA	AES-SHA
AES-SHA	AES-MD5
AES-MD5	AES-MD5
3DES-MD5	AES-MD5
3DES-SHA	AES-MD5
DES-MD5	AES-MD5
DES-SHA	AES-MD5
AES-SHA	3DES-SHA
AES-MD5	3DES-SHA
3DES-MD5	3DES-SHA
3DES-SHA	3DES-SHA
DES-MD5	3DES-SHA
DES-SHA	3DES-SHA
AES-SHA	3DES-MD5
AES-MD5	3DES-MD5
3DES-MD5	3DES-MD5
3DES-SHA	3DES-MD5
DES-MD5	3DES-MD5
DES-SHA	3DES-MD5
AES-SHA	DES-SHA
AES-MD5	DES-SHA
3DES-MD5	DES-SHA
3DES-SHA	DES-SHA

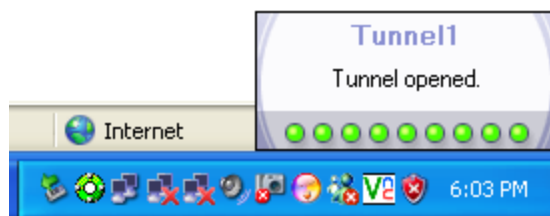
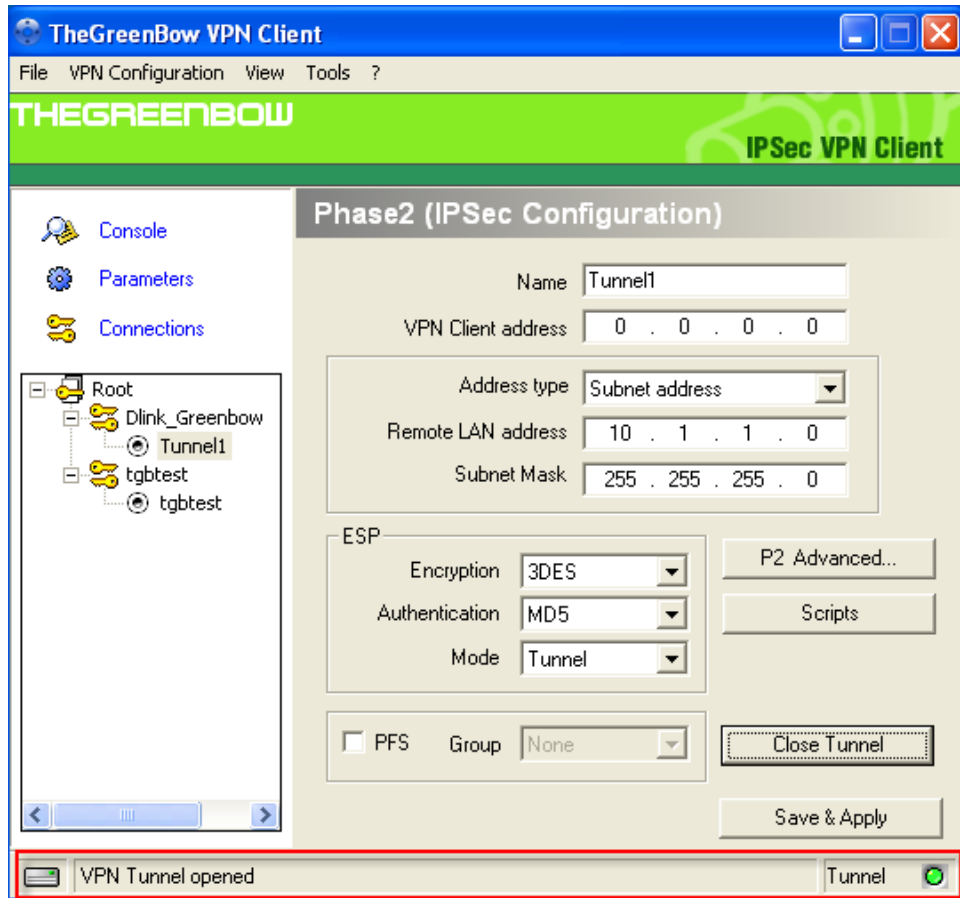
Series Negotiate Mode	
Phase 1	Phase 2
DES-MD5	DES-SHA
DES-SHA	DES-SHA
AES-SHA	DES-MD5
AES-MD5	DES-MD5
3DES-MD5	DES-MD5
3DES-SHA	DES-MD5
DES-MD5	DES-MD5
DES-SHA	DES-MD5

- b. Create users in the WinRadius and during the X-Auth popup, key in the users ID and Password from the WinRadius.



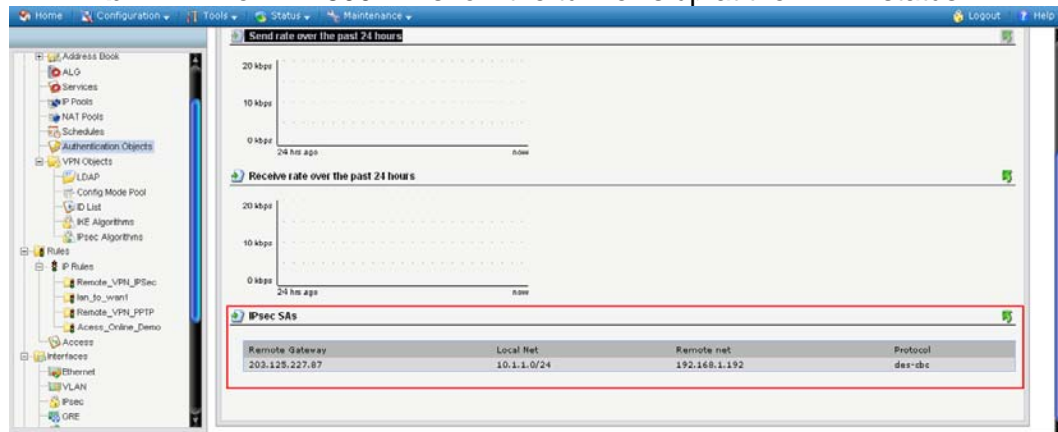
7.2) Test Result

- a. The VPN tunnel will be open at any negotiate mode set in Phase 1 and Phase 2.



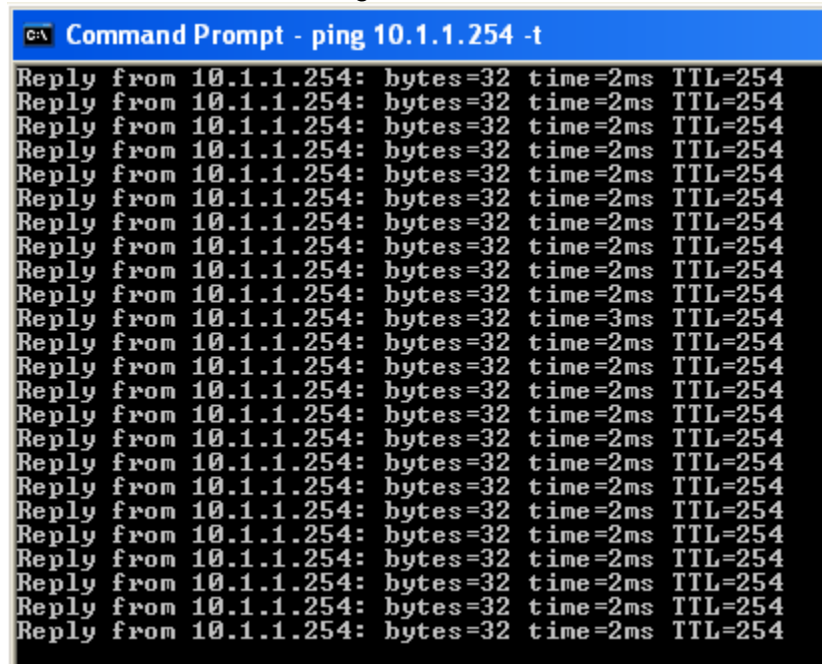
TheGreenBow VPN Client software

b. The DFL-800 will show the tunnel is up at their VPN status.

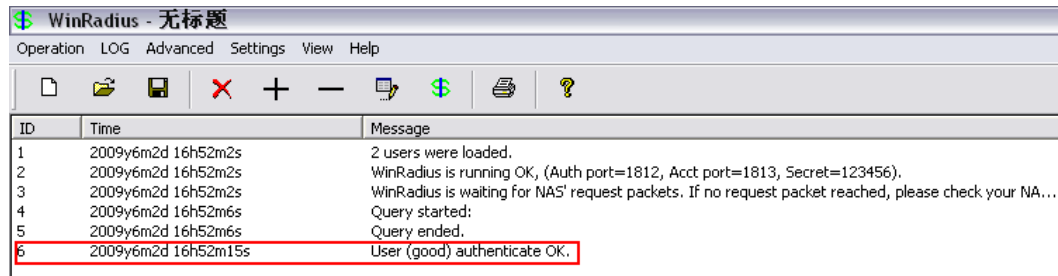


DFL-800 IPSec

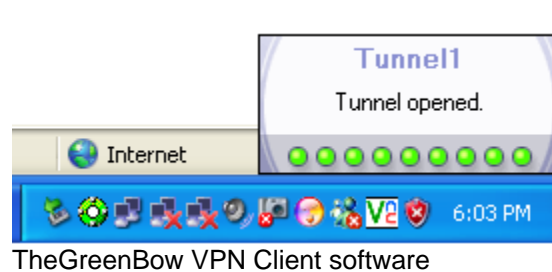
b. Client is able to Ping to the remote network.



- e. For the “X-Auth”, when the valid users are enter in the X-Auth popup. The Radius Server will show “Users Authentication OK” and open up the VPN tunnel.



ID	Time	Message
1	2009y6m2d 16h52m2s	2 users were loaded.
2	2009y6m2d 16h52m2s	WinRadius is running OK, (Auth port=1812, Acct port=1813, Secret=123456).
3	2009y6m2d 16h52m2s	WinRadius is waiting for NAS' request packets. If no request packet reached, please check your NA...
4	2009y6m2d 16h52m6s	Query started:
5	2009y6m2d 16h52m6s	Query ended.
6	2009y6m2d 16h52m15s	User (good) authenticate OK.



8. Conclusion

The Application Notes demonstrate how D-Link VPN products and TheGreenBow VPN software combined perfectly address the requirements of the small and medium businesses worldwide. The joint VPN solution offer advantages around multiple access control and authorization mechanisms for users and tunneling capabilities to access the entire corporate network; it can also provide different access rights to different users.

D-Link Inc. All Rights Reserved

D-Link is the worldwide leader and an award-winning designer, developer, and manufacturer of Wi-Fi and Ethernet networking, broadband, multimedia, voice and data communications and digital electronics solutions.