



D-Link And TheGreenBow Solution

DFL-800 Netdefend IPS/UTM Firewall Application Note

Version 2.01 (2009-10-24)



D-Link International Confidential and proprietary





Revision History

Date	Rev.	Description	Editor
2009-4-24		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		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		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.	

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.



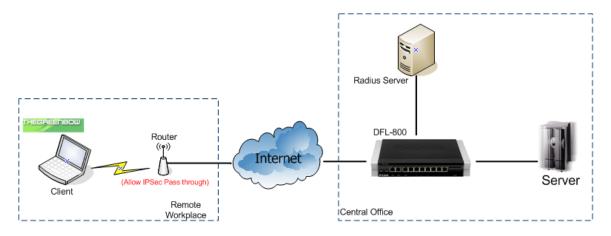


4. List of Equipment and Software

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

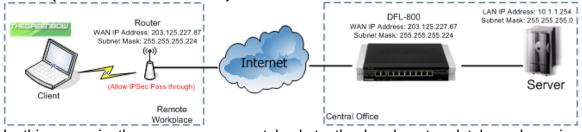
In this document, we will only describe the main configurations for this Scenario. The configurations setting for all the D-Link products will not be described here and for more detail about the product you can download their user guide.

- 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 extra - 2003 125 227 87
🗞 Home 🔌 Configuration - 👔 Tor	ols 🗸 🌀 Status 🗸 🦂 Maintenance 🖌	🙆 Legout 👔 Help
Dijects	PSec-Pre-Shared-Key_1 PSK(the Shared Key) authoritoation to based on a shared secret that is in own only by the parties involved. Ormeral	
Services The Pools The NAT Pools The Schedules Authentication Objects	Name: IPGec-Pra-Shared-Ke	5
Config Mude Pool	© Parsphare Skalad Secret Codim Secret	
Pisc Algorithms	O Hacadeomal Key Pamphara	
Remote_VPN_PSec Remote_VPN_PSec Remote_VPN_PPTP Access_Cnline_Demo	Connerste Random Key Generste Random Key It Since regularwoods and phesos are vulneable 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 ailding Networks for People					Logged in as administrator admin - 203.126.164.157
Home 🛛 📉 Configuration 🚽 🕴	"Tools 🗸 🛛 👩 Status 🗸 🛛 🐜 M	laintenance 🚽			🗳 Logout 🛛 🤶 H
	- 🥂 PH1 3DES-SH/	14			
P Pools	Configure algorithms with		phase of an IPsec s	usion.	
NAT Pools					
Schedules	🛃 General				5
Authentication Objects	Name: PH1_DDES-	SHAL			
LDAP					
Config Mode Pool	Encryption Algorithms	3			5
D List					
KE Algorithms		Preferred	Min	Max	
Psec Algorithms	Null				
-G Rules	DES	64	64	64	
E- S P Rules	D SDES	192	192	192	
Remote_VPN_IPSec Jan_to_wan1	CAST120	128	128	128	
Remote_VPN_PPTP	Blowfish	128	128	448	
Acess_Online_Demo	Twofish				
Access	_	120	120	256	
Chinterfaces	AES (Rijndael)	128 🗸	128	256 🗸	
- Ethernet					 _
-WIVLAN	Integrity Algorithms				<u> 15</u>
- 😚 Psec					
	MD5: 🗹 SHA1:	V			
PPTPA_2TP Servers					
PPTPA_2TP Clients	Comments				
Interface Groups	Comments:				





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

D-Link Building Networks for People						Logged in as administrator admin - 203 126 164 157
🗞 Home 🔰 📉 Configuration 🗸 📔 🎁	Tools 🗸 🧟 Status 🗸 🎭 M	faintenance 🗸				🙆 Logout 🕴 💈 H
1.7	PH2_3DES_ME					
P Pools	Configure algorithms w	hich are used in the IPs	eo phase of an IPseo	session.		
- NAT Pools	D annual					
- Authentication Objects	General					<u>5</u>
- VPN Objects	Name: PH2_3DES	MD5				
LDAP						
	Encryption Algorithm	s				5
- D List						
KE Algorithms		Prefetted	Min	Max		
Psec Algorithms	Null					
3 🥁 Rules	DES	64	84	64		
😑 - 🏮 IP Rules	C SDES	192	192	192		
Remote_VPN_PSec	CAST128	128	128	128		
- 28 Ian_to_wan1 - 28 Remote_VPN_PPTP	Blowfish	120	120			
Acess_Online_Demo				440		
Access	Twofish	120	120	256		
- Chinterfaces	AES (Rijndael)	128	128	v 256 v		
Ethernet					l .	
-ER VLAN	Integrity Algorithms					5
- 😚 Psec						
🠺 GRE	MD5: 🗹 SHA1:					
PPPOE						
PPTPA_2TP Servers	Comments					5
PPTPA_2TP Clients	Comments				1	
Interface Groups						

6.1.1.3) <u>Setting up IPSec-Tunnel</u>

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

D-Link Building Networks for People		dnin - 10.1.1.105
😵 Home 🔰 📉 Configuration 🚽 📲 To	iols 🗸 📔 🧟 Status 🗸 🛛 🐜 Maintenance 🗸	👶 Logout 👔 Help
ALG ALG ALG Photos Photos Autorefication Objects Autorefication Objects Photos	PSec-Tunnel Attractooton XALD Roams RESolutions Resolutions and will appear as a logical intensive in the system. General Advanced Content Authoritocton XALD Roams RESolutions Resolution Advanced Content and Content and	<u>5</u>

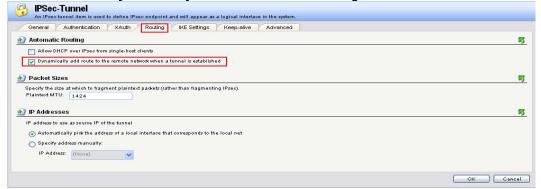




2) Next, click on the "Authentication" tab and select the "Pre-Shared Key" you have setup at the steps 1.

D-Link Building Networks for People		Logged in an administrator admin - 10.1.1.105
🛠 Home 🛛 🖹 Configuration 🗸 📲	Fools 🗸 🤷 Status 🗸 🐂 Maintenance 🖌	👸 Logout 👔 Help
LUAP	Bree-Tunnel An iPsec hannel item is used to define IPsec and point and will appear as a logical interface in	the system.
- Gillo List	Ceneral Authentication XAuth Routing KE Settings Keep-alive A	utvanced
KE Algorithms	Authentication	5
Pade Agreens		
B- B P Rules	X.609 Certificate	
Remote_VPN_PSec	Root Certificate(i): Available Selected	
an_to_want	AdminCart	8
Remote_VPN_PPTP		
Acess_Online_Demo		
Access	44	
Gildertaces		
-118VLAN	T	
- D Psec	Gateway Certificate: (risns)	
- RS ORE	Identification Lat. (Ninna)	
- M PPPoE		
PPTPA_2TP Servers	Pre-shared Key	
PPTPA_2TP Cilerets	Pre-shared Key: IPSec-Pre-Shared- 🗸	
● AR9	Local ID Type: Auto	
E Routing	Local ID Value:	
Ger Authentication		
Contraction	l	
E ZoneDetense		OK Cancel

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.

IPSec-Tunnel An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.	
Ceneral Authentication XAuth Routing IKE Settings Keep-alive Advanced	
<u>ک</u> الاE	疁
Main DH Group Aggressive 2 Perfect Forward Secrecy	5
PFS DH Group	
None 2	



2)



6.1.1.4) <u>Setup IP Rules</u>

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".

D-Link Building Networks for People	Logged in as administrator edmin - 10.1.1.105
🗞 Home 🛛 📉 Configuration 🗸 📲 Tools 🗸 🧑 Status 🗸 🦓 Maintenance 🗸	🚳 Logout 🔰 💈 Help
INAP Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several interfaces for a simplified security pation. Image: Indextance group to combine several	S S OK Carcel
B 3 Traffic Management	

Next, click "IP Rules" and add a new IP rule as show below.

D-Link Building Networks for People		Logged in as administrator admin - 10.1.1.105
😵 Home 🔰 📉 Configuration 🚽 🕴 🎁 To	ols 🗸 🛛 🗧 Status 🗸 🖂 Maintenance 🗸	👸 Logout 🔰 👔 Help
Kome Configuration Configuration Configuration Configuration Configuration Configuration Configuration Configuration Prace Proce Proce	Status Maintenance Comments Comments	Logout P Help
Gradie Construction Gradie Construction Gradie Construction Gradie Construction		OK Cancel





6.1.2) Setup TheGreenBow VPN Client Software

6.1.2.1) <u>Setup Phase 1</u>

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.

🖗 TheGreenBow VPN Client 📃 🗖 🔀			
File VPN Configuration View	Tools ?		
THEGREENBOW			
		IPSec VPN Client	
🚕 Console	Phase1 (Authentication)		
😳 Parameters	Name Dlink_Greenbow		
😂 Connections	Interface Any	-	
Root	Remote Gateway 203.125.227.67		
⊡-S tgbtest	Preshared Key		
Dlink_Greenbow	Confirm:		
	C Certificate Certificates Ir	nport	
	- IKE		
	Encryption 3DES	P1 Advanced	
	Authentication SHA-1		
	Key Group DH2 (1024) 💌		
<		Save & Apply	
VPN ready		Tunnel 🥑	

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





6.1.2.2) <u>Setup Phase 2</u>

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.

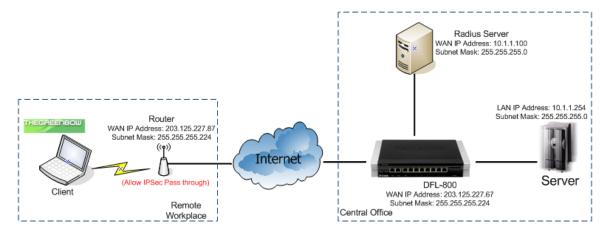
TheGreenBow VPN Clie	ent 📃 🗆 🔀
File VPN Configuration View	Tools ?
THEGREENBOW	
	IP Sec VPN Client
💫 Console	Phase2 (IPSec Configuration)
🛞 Parameters	Name Tunnel1
S Connections	VPN Client address 0 . 0 . 0 . 0
Root	Address type Subnet address Remote LAN address 10 . 1 . 1 . 0 Subnet Mask 255 . 255 . 0
	ESP Encryption 3DES Authentication MD5 Mode Tunnel
	PFS Group None Open Tunnel
<	Save & Apply
VPN ready	Tunnel 🥑

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 \rightarrow 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.

- 🍫 Home 🔰 📉 Configuration 🚽 🛛 🚹 To	ools 🗸 📔 🌏 Status 🗸 🛛 🗞 Maintenance 🗸
DFL-800 DFL-800 DFL-800 DF-66 System De-66 Rules De-67 De-67 PPOE De-67 PTP/L2TP Servers De-67 Rules De-67 PTP/L2TP Clients De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules De-67 Rules Rule	PSec-Tunnel An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system. General Authentication XAuth Routing IKE Settings Keep-alive Advanced IKE XAuth Off Require IKE XAuth user authentication for inbound IPsec tunnels Pass username and password to peer via IKE XAuth, if the remote gateway requires it. Username: Password: Confirm
🗄 🔯 IDP / IPS	

6.2.1.2) <u>Setup the External Authentication Server (i.e. Radius)</u>

1) Add the IP Address for the Radius Server in the "Address Book".

An address folder can be used to group related address objects for better overview.		
All address forder can be dat	a to group related address objects for better overview	
🎦 Add 🗕 🛃 Edit this object		
Name 🚽	Address 👻	
😼 Default_Gateway	203.125.227.65	
🤤 рнср	10.1.1.100-10.1.1.200	
🦁 dmz_ip	172.17.100.254	
🦁 dmznet	172.17.100.0/24	
🤤 DNS_1	165.21.83.88	
🤤 LAN-auth	10.1.1.0/24	
🤤 lan_ip	10.1.1.253	
🤤 lannet	10.1.1.0/24	
🗟 Radius_server	10.1.1.100	
🗟 Remote_net	192.168.1.0/24	
🗟 Subnet	255,255,255.0	
🧟 wan1_ip	203,125,227,67	
🧟 waninet	203,125,227,0/27	
🧟 wan2_ip	192.168.120.254	
🗟 wan2net	192.168.120.0/24	

D-Link International Confidential and proprietary





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

🍣 Home 🔰 📉 Configuration 🚽 🕂 To	ols 🚽 🛛 🕤 Status 🚽	Naintenance 🚽	
PFL-800 System Objects Sector Structure and the fraction Construction Construction Construction Constructure and the fraction Constructure and the fraction	Badius_s(External RADIU:	CIVCI S server used to verify user r	names and passwords.
	Name: IP Address: Port: Retry Timeout: Shared Secret: Confirm Secret:	Radius_server Radius_server I812 2	seconds
	Comments:		

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

3) Next,	add a New	Rule in the "User Authentication Rules".
😙 Home 📉 Configuration 🗸 🎢 To	ools 🗸 📔 🜏 Status 🗸 🛛 🔩	🖕 Maintenance 🗸
PEL-800 System Syste	General Log Settin General Name: Agent: Authentication Source: Interface: Originator IP:	Xauth XAuth





4) At the "Authentication Options", select the Radius Server you have created and select the Radius Method as "CHAP".

General Log S	ettings Authentication Options	Accounting HTTP(s) Agent Option	s PPP Agent Options Restrictions
General			
Select one or more a	uthentication servers. Also select the	e authentication method, which is used for encr	ypting the user p <i>ass</i> word.
Radius Server(s):	Available	Selected	
		Radius_server	
		>>> <	
	-		
		Move up Move down	
Radius Method:	Challenga Handshal 🗸		

 5) Save and activate the setting.
 5) 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 unit material to the unit manually.
 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".

hase1 Advanced	X	
	63)	FF. IPSec VPN Client
Advanced features)
Config Mode Redund.GW	/	enBow
Aggressive Mode NAT-1	Automatic 💌	.182 💌
X-Auth		27.67
X-Auth Popup Logi Hybrid Mode Password		sate Management
Local and Remote ID Choose the type of ID:	Set the value for the ID:	P1 Advanced
Local ID		
Remote ID		
	OK Cancel	Save & Apply
VPN ready		Tunnel 🔮

2) Click "Ok" and "Save & Apply" the setting.





6.2.3) Setup WinRadius Server

6.2.3.1) Set the Secret Key

4 au		<u>.</u>			
Operation	n LOG Advanced	Settings	View	Help	_
	🖻 🖬 💙	System)		\$
		Databa	ase		↓ ↓
ID	Time	Auther	ntication	n	sage
1	2009y6m2d 16h31m	Accour	ntings		ers were l
2	2009y6m2d 16h31m	Logs			Radius is r
3	2009y6m2d 16h31m	Multi-S	ecret		Radius is v
4	2009y6m2d 16h31m	Vertorn	nance		son: Unkn
5	2009y6m2d 16h31m	renon	nanco.		i (hi) authi
6	2009y6m2d 16h31m	21s		Use	r (test) au
7	2009y6m2d 16h31m	135s		Que	ery started
8	2009y6m2d 16h31m	135s		Que	ery ended.
1					

2) Key in the "NAS Secret".

System settings		×
NAS Secret:	123456	
Authorization port:	1812	
Accounting port:	1813	
Launch when system startups		
Minimize the application when startups		
ОК		Cancel

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 Mo	de
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.

GreenBow VPN Clie	ent	
File VPN Configuration View	Tools ?	
THEGREENBOW	Trace Mode is ON. Press Ctrl+Alt+D to Trace OFF.	IPSec VPN Client
🔑 Console	Phase2 (IPSec Configurat	ion)
Parameters	Name Tunnel1	
S Connections	VPN Client address 192	168 . 1 . 182
Dlink_GreenBow-P1	n login and password to open the tunnel.	ddress Image: Constraint of the second sec
<	OK Cancel	Open Tunnel <u>S</u> ave & Apply
Opening Tunnel	Phase 1 (ID)	Tunnel 🥑





7.2) **Test Result**

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

TheGreenBow VPN Clie	ent 🔲 🗖 🗙
File VPN Configuration View	Tools ?
THEGREENBOW	IPSec VPN Client
🔑 Console	Phase2 (IPSec Configuration)
Parameters	Name Tunnel1
S Connections	VPN Client address 0 . 0 . 0 . 0
Root	Address type Subnet address Remote LAN address 10 . 1 . 1 . 0 Subnet Mask 255 . 255 . 0 ESP Encryption 3DES Authentication MD5 Mode Tunnel
	PFS Group None Close Tunnel
<	Save & Apply
VPN Tunnel opened	Tunnel 🖸
	T



TheGreenBow VPN Client software





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

	Send rate over the past 24 hours				
Address Book ALG Services P Pools NAT Pools	20 Mbpu 10 Mbpu				
Schedules Authentication Objects	0 kbpr				
VPN Objects	24 her apo	n.com			
10 LDAP	Receive rate over the past 24 hours				
E D List KE Algorithms Ke Algorithms Sec Algorithms As P Rules Remote_VPN_PSec Inn jo_wani	20 kbps 10 kbps 0 kbps 24 hm aps				
Acess_Online_Demo	1 IPsec SAs				5
Access	Remote Gateway	Local Net	Remote net	Protocol	
erfaces Ethernet	203.125.227.87	10.1.1.0/24	192.168.1.192	des-cbc	
VLAN Psec ORE					

DFL-800 IPSec

- Command Prompt ping 10.1.1.254 -t bytes=32 time=2ms time=2ms time=2ms Reply from Reply from Reply from from 10.1.1.254: from 10.1.1.254: from 10.1.1.254: from 10.1.1.254: Reply time=2ms time=2ms time=2ms 10.1.1.254: from Reply TTT. from 10.1.1.254: Reply time=2ms time=2ms time=2ms from 10.1.1.254: Reply 254: 10.1.1. from eply eply from 10.1.1. 254: bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 time=2ms -1 from 254: Reply 10.1 time=3ms time=2ms time=2ms Reply Reply from 10.1.1 254: from 10.1.1. 254: Reply .1 from 10.1 54: time=2ms time=2ms time=2ms Reply from 10.1.1 254: from 10.1.1 254: Reply Reply from 10.1.1 4: bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 bytes=32 time=2ms time=2ms time=2ms time=2ms time=2ms time=2ms time=2ms time=2ms Reply from 10.1 -1 254: leply from 10.1 .1 4: Reply from 10.1.1. 4: -1 from Reply 10.1 4: from 10.1.1 leply 4: from 10.1.1. 254: Reply 4 Reply from 10.1.1. 4: bytes=32 time=2ms Reply from 10.1.1.254: 54 ТΤ
- **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.

Operati	ion LOG Advanced Settings View	Help			
D	🛎 🖬 🗙 🕂 -	- 🗊 💲 🏻 🚭 🖓			
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.			



TheGreenBow VPN Client software





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.