



### **D-Link And TheGreenBow Solution**

# Netdefend IPS/UTM Firewall Application Notes

Version 1.01 (24 / 10 / 2009)





### **Revision History**

Date	Rev.	Description	Editor
		Interoperability Compliance Testing Negotiate mode for	
24/04/2009	1.0	Phase1 and Phase2 using TheGreenBow VPN Client and D-	John Yoong
		Link product's DFL-800.	_
		Changing DFL-800 firmware from 2.20.00 to 2.26.00.06 and	
24/10/2009	1.01	TheGreenBow VPN Client firmware 4.60.00 to 4.61.003 and	John Yoong
		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 program, 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	-	4.61.003
2	Netdefend IPS firewall	DFL-800	2.26.00.06-12649





### 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.

### 6.1 TheGreenBow VPN client and D-Link security solutions



In this scenario the user can connect back to the headquarter database by using TheGreenBow VPN client tunneling 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
  - Setup Phase 1
  - Setup Phase 2

D-Link International Confidential and proprietary





### 6.1.1) Setup DFL-800 for VPN tunneling

### 6.1.1.1) <u>Setup Pre-Shared Key</u>

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 - 2003.125.227.07
🗞 Home 🔌 Configuration 🚽 🏦 Tools	🔹 😘 Status 🗸 🐴 Maintenance 🗸	🔓 Legout 🔰 🛔 Help
Objects     B Address Book     Address Book	PSE(Pre-Shared-Key_1           PSE(Pre-Shared Key) anthenkaatsin is based on a shared secret that is innown only by the parties involved.           () General	
Services Services Services NAT Pools Pol	Name: [[PSec-Pre-Shared-Ke] @) Shared Secret	5
Config Mude Pool	Pasphase     Stated Secret     content execute	
Pisc Algorithms	C Hexdeomal Key Pamphana	
Renote_VPN_IPSec     Renote_VPN_IPSec     Renote_VPN_IPTP     Access_Online_Demo	Generate Random Key	

### 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.

<b>D-Link</b> Building Networks for People					Logged in as administrator admin - 203.128.164.167
- 🗞 Home 🔰 📉 Configuration 🚽 🛛 👖 T	'ools 🗸 📔 👩 Status 🗸 🛛 🎭 M.	sintenance 🚽			😚 Logout 🔰 Hel
P Pools	Configure algorithms whi	1 ch are used in the IKE	phase of an IPsec se	ssion.	
Authentication Objects	Name: PH1_3DE5-5	HAI			<u>5</u>
KE Algorithms     Psec Algorithms	Null	Preferred	Min	Max	
- \$ IP Rules	V ves	04	04	04	
- Call Remote_VPN_IPSec	CAST120	192	192	192	
-C Remote_VPN_PPTP	Blowfish	128	128	448	
Acess_Online_Demo	Twofish	120	120	256	
E Chinterfaces	AES (Rijndael)	128 🗸	128	256 🗸	2
- Ethernet - EVLAN	Integrity Algorithms				
Psec     Re     PPTPL2TP Servers     PPTPL2TP Servers	MD5: 🗹 SHA1:				7
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					Loggend in as administrator admin - 203 126 164 157
🐟 Home 🕴 💐 Configuration 🗸 🍴 👬 T	'ools 🗸 📋 👩 Status 🗸 📔 🔩 M	aintenance 🚽			👶 Logout 🛛 🐉 Help
P Pools	Configure algorithms wh	5 ich are used in the IPse	ophase of an IPsec	session.	
Schedules     Schedules     VPN Objects     VPN Objects	General     Name:     PH2_3DES_N	MD5			<u> </u>
	Encryption Algorithms				<b>I</b> <u>5</u>
- ElD List - BE Algorithms - Psec Algorithms	Null	Preferred	Min	Max	
E 🙀 Rules	DES	64	64	64	
B- § P Rules	I SDES	192	192	192	
lan to want	CAST128	128	128	128	
Remote_VPN_PPTP	Blowfish	120	120	440	
Acess_Online_Demo	Twofish	120	120	256	
- Access	AES (Rijndael)	128 🗸	128	256 🗸	
Ethernet	-				
-WVLAN	Integrity Algorithms				町
- 😚 Psec					
- 000 AE	MD5: 🗹 SHA1:	✓			
PPTPL2TP Servers	D Commente				-
PPTPA_2TP Clients	Comments				<u> </u>
Interface Groups	Comments:				

### 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		Logged in as administrator admin - 10.1.1.105
🗞 Home 🛛 🖹 Configuration 🗸 🕴 👬 T	'ools 🗸 🛛 🚭 Status 🗸 🖂 Maintenance 🗸	🔓 Logout 🕴 💈 Help
ALO Services WATPods NATPods NATPods Authentication Objects WATHENDARK Authentication Objects WATHENDARK Remote, VTNL PSec Inn Jo, want Remote, VTNL PSec Inn Jo, want Inn Jo, want Remote, VTNL PSec Inn Jo, want Remote, VTNL PSec Inn Jo, want Inn Jo, want	PSec-Turnel     Alfretoution     Advanced     Presented     Advanced     Advan	<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		drin - 10.1.1.105
S Home 🛛 Configuration - 📲	Tools 🗸 👩 Status 🗸 🔸 Maintenance 🗸	👸 Logout 👔 Help
LUAP	Bree-Tunnel An iPeer tunnel item is used to define iPeen andpolet and will appear as a topical interface in the system.	
- Elip List	General Authentication XAuth Routing KE Settings Keep-alive Advanced	
- KE Algorithms		
Psec Algorithms	*/ Authentication	<u>19</u>
E G Rules		
B- S P Rules	O X.609 Cedificate	
Remote_VPN_PSec	Root Certificate(x): Available Selected	
an_to_wan1	AdminCart A	
Remote_VPN_PPTP		
Acess_Online_Demo	22	
Access		
E-us/sterfaces		
Ethernet	8 8	
- LIPVLAN	Outeway Certificate: (Pinna)	
di non-r	Identification Lut: (Finna)	
ODDTDA OTD Carriers	Pre-shared Key	
- C PRTPA TTP Charte	Preshared Key IDSac - Dras Shareds and	
The Interface Groups	L'ESCHIC CHILD	
- ADD		
H-GARouting	Alto Y	
E CP/PS	Local ID Value:	
User Authentication		
Trattic Management		- <u></u>
R D 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 Client.

General       Authentication       XAuth       Routing       IKE         IKE       IMain       DH Group       IMain       IMain         Aggressive       2       Imain       Imain       Imain         Perfect Forward Secrecy       Imain       Imain       Imain       Imain         PFS       DH Group       Imain       Imain	IPSec-Tunnel An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.	
INE       Image: Main       OH Group       Aggressive       2       Perfect Forward Secrecy       PFS       DH Group	General Authentication XAuth Routing IKE Settings Keep-alive Advanced	
Main DH Group     Aggressive 2 Perfect Forward Secrecy PFS DH Group	) IKE	
Perfect Forward Secrecy PFS DH Group	Main DH Group     Aggressive 2	
PFS DH Group		
	PFS DH Group	





#### 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 admin - 101.1.105
- 🥱 Home 🛛 🖹 Configuration 🗸 🛛 👬	Tools 🗸 📲 Status 🖌 🍓 Maintenance 🗸	😚 Logout 🕴 🍞 Help
Config Mode Pool	IPSec-LAN Use an interface group to combine several interfaces for a simplified security policy.	
KE Algorithms	🛃 General	<b>15</b>
Perc Alporthms  Alport Parce Alporthms  Parce Alport Par	Name: IPSec-LAN GenothyTransport Equivalent interfaces Facilitation Form	<u>17</u>
- te PPPoE	Comments	5
PPTPA_2TP Servers PPTPA_2TP Clents Interface Groups AR9 Reference Groups	Commente	~~~~~
E DP / PS		
User Authentication		OK Cancel
FI-23 Traffic Management		

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

D-Link Building Networks for People		Logged in as <b>administrator</b> admin - 10.1.1.105
- 😚 Home 🔰 🎇 Configuration 🚽 🛛 👬 T	ools 🗸 🛛 🚘 Status 🗸 🛛 💑 Maintenance 🗸	🗳 Logout 🛛 💈 Help
Config Mode Pool	PSec-Allow As the specifies what action to perform on network traffic that matches the specified filter orderia.	
KE Algorithms	General     General     General	<u>15</u>
Rules     Rende_VPN_PSec     Imn_to_wan1     Rende_VPN_PTP	Name:     [PSec-Allow]       Action:     Allow       Schodvid:     all_republicmp       Schodvid:     Otom	
Access_Online_Demo	Address Filter      Specify source Interface and Source network, together with destination interface and destination network. All parameters have to match for the rule to match.	
- WYLAN - S Piec - S GRE - PPPOE - PPTA 2TP Servers	Source Destination Interface: Network: all-nets v	
PPTPL_2TP Clients	Comments Comments	<u> 15</u>
CP / IPS     User Authentication     User Authentication     User Authentication     User Authentication     User Authentication     User Authentication     User Authentication		OK Cancel





### 6.1.2) Setup TheGreenBow VPN Client

### 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 Clier	nt 🔳	
File VPN Configuration View	Tools ?	
THEGREENBOW		
	IPSec VPN	Client
🚕 Console	Phase1 (Authentication)	
Parameters	Name Dlink_Greenbow	
😂 Connections	Interface Any	
	Remote Gateway 203.125.227.67	
ergetest	Preshared Key	
Tunnel1	Confirm: ******	
	C Certificate Certificates Import	
	IKE R1 A L	- 1
	Encryption 3DES	:d
	Authentication SHA-1	
	Key Group DH2 (1024)	
<	Save & App	ply
VPN ready	Tunr	nel 🕑

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		IDEas VDN Client
		IF SEC VEN CHERT
💫 Console	Phase2 (IPSec Configuration)	)
🛞 Parameters	Name Tunnel1	
😂 Connections	VPN Client address 0 . 0	. 0 . 0
Root Contemporation Contempo	Address type Subnet address Remote LAN address 10 . 1 Subnet Mask 255 . 255	s <b>-</b> . 1 . 0 . 255 . 0
	ESP Encryption 3DES Authentication MD5 Mode Tunnel	P2 Advanced Scripts
	FFS 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.





### 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
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

### 7.2) Test Result

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

TheGreenBow VPN Clie	ent 📃 🗖 🗙
File VPN Configuration View	Tools ?
THEGREENBOW	
	IPSec VPN Client
🔑 Console	Phase2 (IPSec Configuration)
🚱 Parameters	Name Tunnel1
😂 Connections	VPN Client address 0 . 0 . 0 . 0
Root Contempose	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 🧿







TheGreenBow VPN Client

#### **b.** The DFL will show the tunnel is up at their VPN status.

P Markets Block     20 Mays       Services     P Pool       Services     P Pool       WH Pool     Services       Outpy     Advance       Services     P Pool       Outpy     Advance       Services     P Pool       Services     Pool       Services     Pool       Services     County       Services     County       Services     Pool       Services     County       Services     County       Services     County       Services     Services       Services     County       Services     County       Services     County       Services     County       Services     County       Services     Services	over the past 24 hours	,
VPN Genets     20 km api     som       LDAP     Bacebox rate over the past 24 hours       Config Mode Pool     Image       Config Mode Pool     20 km api       De Agostrins     20 km api       De Daystrins     10 kpe       P Revelow coller     20 km api       P Revelow coller     0 kpe       P Revelow coler     0 kpe		
Image: Config Mode Pool     Image: Pool of P	J ago now	
Condy Mode Pool     Circle Mode Pool     Condy Mode Pool     Condy Mode Pool     Condy     Condy Mode Pool     Condy	te over the past 24 hours	
L Remote VPL/Sec Sen_D_went Sen_D_went I Remote VPL/SPP Access Remote Gateway Construction Remote Gateway Local Net Remote Gateway Remote Gate		
Alen_D_vent      Arms agr      two     Access     Crime Demo     Access     Accees     Access     Access     Access     Access     Access     Acc		
Access, Order, Deno     A	1920 0000	
Access Access Remote Gateway Local Net Remote net Protocol risces 200.135.227.87 10.1.1.0/24 192.145.1.192 de-de-		
rfaces Remote Gateway Local Net Remote net Protocol 200.125.227.07 10.1.1.0/24 192.168.1.192 des-thr		
203.125.227.87 10.1.1.0/24 192.168.1.192 dec-dec	rtevay Local Net Remote net	Protocol
Ethernet	17.87 10.1.1.0/24 192,168.1.1	.92 des-cbc
TVLAN		

DFL-800 IPSec

🔤 Command F	Prompt - ping	10.1.1.254	-t	
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	LØ.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	LØ.1.1.254:	bytes=32	time=3ms	TTL=254
Reply from 1	LØ.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	LØ.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	LØ.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	LØ.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	10.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	0.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	0.1.1.254:	bytes=32	time=2ms	TTL=254
Reply from 1	0.1.1.254:	bytes=32	time=2ms	TTL=254

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





### 8. Conclusion

The Application Notes demonstrate how D-Link VPN products and TheGreenBow 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.