Configuring TheGreenBow VPN Client with a TP-LINK VPN Router

This chapter describes how to configure TheGreenBow VPN Client with a TP-LINK router. This chapter includes the following sections: **Example VPN Network Topology**, **Configure the TP-LINK VPN Router**, **Configure TheGreenBow VPN Client**.

1.1 Example VPN Network Topology

In the VPN network example shown in the figure below, the VPN router functions as a gateway for a main office. The Windows PC VPN Client is installed on a remote laptop that runs Windows XP and that connects to the Internet. The Windows PC VPN Client connects to the VPN router and establishes a secure IPSec VPN connection with the router so the laptop user can gain access to the file server or any other resources at the main office.



Figure 7-1

The following table shows the IP addresses that are used in the VPN network example shown in

```
Figure 7-1.
```

Main Office	Remote Home Office
Main office router:	Home office router:
WAN IP: 110.200.13.18	Windows XP laptop with VPN Client:
□VPN Router IP address: 192.168.0.1	116.31.85.133
□Subnet mask: 255.255.255.0	Subnet mask: 255.255.255.0
	□Default gateway: 116.31.85.1

File server IP: 192.168.0.2	VPN Client settings:
Subnet mask: 255.255.255.0 □	Pre-shared key:123456
Default gateway: 192.168.0.1	
Client IP: 192.168.0.3	
Subnet mask: 255.255.255.0□	
Default gateway: 192.168.0.1	

A Note:

All the addresses in this chapter are for example only. You can adjust the settings and configuration to suit your network.

1.2 Configuring the TP-LINK VPN Router

To configure a VPN connection between the VPN router and a client, access the router's Web management interface, create an IKE policy, and then create a VPN policy.

1) IKE Setting

To configure the IKE function, you should create an IKE Proposal firstly.

IKE Proposal

Choose the menu $VPN \rightarrow IKE \rightarrow IKE Proposal$ to load the configuration page.

Settings:

Proposal Name:	proposal_IKE_1
Authentication:	MD5
Encryption:	3DES
DH Group:	DH2

Click the <Add> button to apply the setting.

IKE Proposal		
Proposal Name:	proposal_IKE_1	
Authentication:	MD5	
Encryption:	3DES 💌	н
DH Group:	DH2	



• IKE Policy

Choose the menu $\textbf{VPN} {\rightarrow} \textbf{IKE} \ \textbf{Policy}$ to load the configuration page.

Settings:

Policy Name:	IKE_1
Exchange Mode:	Main
IKE Proposal:	proposal_IKE_1 (you just created)
Pre-shared Key:	123456
SA Lifetime:	28800
DPD:	Disable

Click the <Add> button to apply.

IKE Policy			
Policy Name:	IKE_1		
Exchange Mode:	Main Aggressive Clear		
Local ID Type:	IP Address FQDN Help		
Local ID:	Local WAN IP		
Remote ID Type:	⊙ IP Address ○ FQDN		
Remote ID:	Remote Gateway IP		
IKE Proposal 1:	proposal_IKE_1 💙		
IKE Proposal 2:	v		
IKE Proposal 3:	v		
IKE Proposal 4:	💌		
Pre-shared Key:	123456		
SA Lifetime:	28800 Sec (60-604800)		
DPD: 🔿 Enable 💿 Disable			
DPD Interval:	15 Sec (1-300)		
List of IKE Policy			
No. Name	Mode Proposal 1 Proposal 2 Proposal 3 Proposal 4 Action		
	No entries.		
Select All Delete Search			

Figure 7-3

2) IPsec Setting

To configure the IPsec function, you should create an IPsec Proposal firstly.

• IPsec Proposal

Choose the menu $VPN \rightarrow IPsec \rightarrow IPsec Proposal$ to load the following page.

Settings:

- Proposal Name: proposal_IPsec_1
- Security Protocol: ESP
- ESP Authentication: MD5
- ESP Encryption: 3DES

Click the <Save> button to apply.

IPsec Proposal		
Proposal Name:	proposal_IPsec_1	
Security Protocol:	ESP	Add
ESP Authentication:	MD5 💌	Clear
ESP Encryption:	3DES 💌	Help



• IPsec Policy

Choose the menu $\textbf{VPN} {\rightarrow} \textbf{IPsec} {\rightarrow} \textbf{IPsec}$ policy to load the configuration page.

Settings:

IPsec:	Enable
Policy Name:	IPsec_1
Status:	Activate
Mode	Client-to-LAN
Local Subnet:	192.168.0.0/24
WAN:	WAN1
Remote Host:	116.31.85.133
Exchange Mode	IKE
IKE Policy:	IKE_1
IPsec Proposal:	proposal_IPsec_1 (you just created)
PFS:	NONE
SA Lifetime:	3600

Click the <Add> button to add the new entry to the list and click the <Save> button to apply.



It is suggested to set the Remote Host to be 0.0.0.0, which means there is no limit to the IP address of the remote host with VPN Client.

TD					
IPsec:	💿 Enable 🔘 Disable				Save
Psec Policy					
Policy Name:	IPsec_1				(Add
Mode:	Client-to-LAN 💙				Clear
Local Subnet:	192.168.2.0 / 24				Help
Remote Subnet:	0.0.0.0 / 0				
WAN:	WAN1 💌				
Remote Host:	116.31.85.133				
Policy Mode:	💿 IKE 🔘 Manual				
IKE Policy:	IKE_1				
IPsec Proposal 1:	proposal_IPsec_1 💌				
IPsec Proposal 2:	💌				
IPsec Proposal 3:	💌				
IPsec Proposal 4:	💌				
PFS:	NONE				
SA Lifetime:	3600 Sec (120-6	04800)			
Status:	💿 Activate 🔘 Inactivate				
ist of IPsec Policy					
No. Name	Mode Local Subnet	Remote Subnet	Policy Mode	Status	Action
	No e	ntries.			
Select All Activate Delete Search					



1.3 Configuring TheGreenBow VPN Client

TheGreenBow VPN Client lets you to set up the VPN connection manually or with the integrated Configuration Wizard, which is the easier and preferred method. The Configuration Wizard uses the default settings and provides basic interoperability so that TheGreenBow VPN Client can easily communicate with TP-LINK or third-party VPN devices. However, the Configuration Wizard does not let you enter the local and remote IDs, so you must manually enter this information.

1.3.1 Use the Configuration Wizard to Configure TheGreenBow VPN Client

 Access TheGreenBow VPN Client's user interface, and select VPN Configuration > Wizard from the main menu on the Configuration Panel screen. TheGreenBow VPN Client Configuration Wizard Step 1 of 3 screen displays.



Figure 7-6

2. Select the **A router or a VPN gateway** radio button, and click Next. TheGreenBow VPN Client Configuration Wizard Step 2 of 3 screen displays.

VPN Configuration Wizard	
VPN tunnel parameters	2/3
Enter the following parameters for the VPN	tunnel:
IP or DNS public (external) address: of the remote equipment	110.200.13.18
Preshared-key:	•••••
IP private (internal) address: of the remote network	192 . 168 . 0 . 0
< Previous	Next > Cancel

Figure 7-7

3. Specify the following VPN tunnel parameters:

IP or DNS public (external) address of the remote equipment: Enter the remote IP address or DNS name of the VPN router: 110.200.13.18.

Preshared-key: Enter 123456, which is the preshared key that you already specified on the VPN router.

IP private (internal) address of the remote network: Enter 192.168.0.0, which is the remote private IP address of the remote VPN router. This IP address enables communication with the entire 192.168.0.x subnet.



All the addresses in this chapter are for example purposes only. You can adjust the settings and configuration to suit your network.

4. Click **Next**. TheGreenBow VPN Client Configuration Wizard Step 3 of 3 screen displays.

VPN Configuration Wizard	×
Configuration Summary 3/3	
The tunnel configuration is correctly completed : Tunnel name: Gateway Remote Equipment: Router or VPN gateway IP or name of this equipment: 110.200.13.18 Preshared key: ****** IP address of the remote network: 192.168.0.0 Subnet mask: 255.255.0.0	
You may change these parameters anytime directly with the main interface.	
< Previous Finish Cancel	

Figure 7-8

- 5. This screen is a summary screen of the new VPN configuration. Click Finish.
- 6. Specify the local and remote IDs:
 - a) Click on the default name Gateway1 in the tree list window of the Configuration Panel screen.
 The Phase 1 (Authentication) window displays in the Configuration Panel screen.
 - b) Click **Advanced**. The Phase 1 Advanced screen displays.

TheGreenBow IPSec VPN Clie	ent 🔳 🗖 💟
Configuration Tools ?	
THEGREENBOW	IPSec VPN Client
Save Apply	Authentication Advanced Certificate Advanced features Mode Config Redun. GW Aggressive Mode NAT-T Authentication Value for the ID:
	Local ID V
VPN Client ready	

Figure 7-9

c) Specify the settings that are explained in the following table.

Setting	Description
Aggressive Mode:	Enable or disable aggressive mode as the negotiation mode with the VPN router.
NAT-T:	Select Automatic from the drop-down list to enables TheGreenBow VPN Client and VPN router to negotiate NAT-T. It is suggested to enable it.
Local ID:	As the type of ID, select DNS from the Local ID drop-down list if you specified FQDN in the VPN router configuration or select the IP Address if you specified IP Address in the VPN router configuration. The VPN router only supports IP Address and DNS.
Remote ID:	As the type of ID, select DNS from the Remote ID drop-down list if

you specified FQDN in the VPN router configuration or select the IP
Address if you specified IP Address in the VPN router configuration.
The VPN router only supports IP Address and DNS.

- d) Click **OK** to save the settings.
- 7. Specify the global parameters:
 - a) Select VPN Configuration > Parameters from the main menu. The Parameters window is displayed in the Configuration Panel screen.

🗟 TheGreenBow IPSec VPN Client 📃 🗖 🔀					
Configuration Tools ?					
THEGREENBOW					
					N Client
				P Sec VP	N Ghent
Save Apply	Global Parameters				
E VPN Configuration	Global Parameters				
Global Parameters	Lifetime (sec.)				
in O Tunnel		Default	Minimal	Maximal	
of tgbtest	Authentication (IKE)	28800	360	28800	
_	Encryption (IPSec)	3600	300	28800	
	Dead Peer Detectio Check interval Max. number of retries Delay between retries Miscellaneous Retransmissions X-Auth timeout	n (DPD) 30sec 5 15sec 2 60 Disable Sp	IKE Po NAT Po NIt Tunneling	rt	
VPN Client ready					

Figure 7-10

- b) Specify the default lifetimes in seconds:
 - Authentication (IKE), Default: The default lifetime value is 3600 seconds. Replace this setting to 28800 seconds to match the configuration of the VPN router.
 - Encryption (IPSec), Default: The default lifetime value is 1200 seconds. Replace this setting to 3600 seconds to match the configuration of the VPN router.
- c) Click Save.

TheGreenBow VPN Client configuration is now complete.

To connect TheGreenBow VPN Client to the VPN router, see Establish a VPN connection.

1.3.2 Manually Configure TheGreenBow VPN Client

To manually configure a VPN connection between TheGreenBow VPN Client and a router, access TheGreenBow VPN Client's user interface, create an IKE phase 1 configuration, an IPSec phase 2 configuration, and then specify the global parameters.

To set up an IKE phase 1 configuration:

1. Right-click on 'VPN Configuration" in the tree list window and select 'New Phase 1'.



Figure 7-11

2. The Phase 1 (Authentication) window displays in the Configuration Panel screen.

TheGreenBow IPSec VPN Clie	nt	
Configuration Tools ?		
THEGREENBOW		
		IPSec VPN Client
		I See VI II Sherr
Save Apply	Gateway: Authentical	tion
YPN Configuration	Authentication Advanced Certifi	cate
Global Parameters	Addresses	
	Interface	116.31.85.133 👻
	Remote Gateway	110.200.13.18
	Authentication ————	
	💿 Preshared Key	•••••
	Confirm	•••••
	🔘 Certificate	
	ІКЕ	
	Encryption	3DES 💌
	Authentication	MD5 🗸
	Key Group	DH2 (1024) 🗸
VPN Client ready		

Figure 7-12

3. Specify the settings that are explained in the following table.

Setting	Description			
Interface:	Select the IP A	Select the IP Address of the home office router from the drop-down list.		
Remote Gateway:	Enter the remote IP address of the VPN router: 110.200.13.18.			
Preshared Key:	Select the Preshared Key radio button. Enter 123456, which is the preshared key that you already specified on the VPN router. Confirm the key in the Confirm field.			
Encryption Select the 3DES encryption algo list.		Select the 3DES encryption algorithm from the drop-down list.		
	Authentication	Select the MD5 authentication algorithm from the		

	drop-down list.
Key Group	Select the DH2 (1024) key group from the drop-down list.



The IKE Proposal you created for TheGreenBow VPN Client must be the same as the Proposal on the VPN router.

- 4. Click **Save** to save the settings.
- 5. On the same screen, click **Advanced** The Phase 1 Advanced screen displays.

🗟 TheGreenBow IPSec VPN Client 📃 🗖 🔀			
Configuration Tools ?			
THEGREENBOW			
	IPSec VPN Client		
Save Apply	tgbtest: Authentication		
VPN Configuration	Authentication Advanced Certificate		
Global Parameters	Advanced features		
	Mode Config Redun. GW		
On typicest	Aggressive Mode NAT-T Automatic		
	X-Auth		
	X-Auth Popup Login		
	Hybrid Mode Password		
	Local and Remote ID		
	Type of ID: Value for the ID:		
	Local ID		
	Remote ID		
• VPN Client ready			

Figure 7-13

6. Specify the settings that are explained in the following table.

Setting	Description
Setting	Description

Aggressive Mode:	Enable or disable aggressive mode as the negotiation mode with the VPN router.
NAT-T:	Select Automatic from the drop-down list to enables TheGreenBow VPN Client and VPN router to negotiate NAT-T.
Local ID:	As the type of ID, select DNS from the Local ID drop-down list if you specified FQDN in the VPN router configuration or select the IP Address if you specified IP Address in the VPN router configuration. The VPN router only supports IP Address and DNS.
Remote ID:	As the type of ID, select DNS from the Remote ID drop-down list if you specified FQDN in the VPN router configuration or select the IP Address if you specified IP Address in the VPN router configuration. The VPN router only supports IP Address and DNS.

7. Click **Save** to save the settings.

To set up an IPSec phase 2 configuration:

1. Right-click on the new Phase 1 in the tree control and select "New Phase 2'.





2. Click on the new Phase 2 in the tree control, the Phase 2 (IPSec Configuration) screen displays.

Establish a VPN connection

TheGreenBow IPSec VPN Clie	nt	
Configuration Tools ?		
THEGREENBOW		IPSec VPN Client
Save Apply	Tunnel: IPSec	
VPN Configuration	IPSec Advanced Scripts Remote Shar	ing
Global Parameters	Addresses	
O Tunnel	VPN Client address	116 . 31 . 85 . 133
	Address type Su	ibnet address 🔽
	Remote LAN address	192 . 168 . 0 . 0
	Subnet mask 2	255 . 255 . 255 . 0
	ESP	
	Encryption 3D	DES 💌
	Authentication M	05 🗸
	Mode Tu	innel 🔽
	PFS	
	PFS Group	×
VPN Client ready		

Figure 7-15

3. Specify the settings that are explained in the following table.

Setting	Description
VPN Client address:	It is suggest keeping 0.0.0.0 in this field. You can also enter the IP address of the host with VPN Client, but the IP address cannot be the same as the interface IP address of the VPN router or belong to the remote subnet.
Address Type:	You can only select the Subnet address type.
Remote LAN Address:	Enter 192.168.0.0 as the remote IP address. It must be the same as the LAN address of the remote VPN router.
Subnet Mask:	Enter 255.255.255.0 as the remote subnet mask of the gateway that opens the VPN tunnel. It must be the same as the Local Subnet set in the VPN router.

	Encryption	Select 3DES as the encryption algorithm from the drop-down list.
ESP:	Authentication	Select MD5 as the authentication algorithm from the drop-down list.
	Mode	Select Tunnel as the encapsulation mode from the drop-down list. TheGreenBow VPN Client supports Tunnel Mode only.

4. Click the **Save**.

There are more options within **P2 Advanced**, however for this document we won't be going into these features.

Global parameters

1. Select VPN Configuration > Parameters from the main menu. The Parameters window displays in the Configuration Panel screen.

TheGreenBow IPSec VPN Client					×
Configuration Tools ?					
THEGREENBOW				IPSec VPN Clie	nt
Save Apply	Global Parameters				
VPN Configuration	Global Parameters				
Gateway	Lifetime (sec.)				
	Authentication (IKE)	Default 28800	Minimal 360	Maximal 28800	
IIIII OT tgbtest	Encryption (IPSec)	3600	300	28800	
	Dead Peer Detectio	on (DPD) —	-		
	Max. number of retries	5			
	Delay between retries	15 sec	:.		
	Miscellaneous				
	Retransmissions	2	IKE Po	ort	
	X-Auth timeout	60	NAT Po	ort	
	Disable Split Tunneling				
VPN Client ready	•				j

- 2. Specify the default lifetimes in seconds:
 - Authentication (IKE), Default: The default lifetime value is 3600 seconds. It is suggested to keep the default value.
 - Encryption (IPSec), Default: The default lifetime value is 1200 seconds. It is suggested to keep the default value.
- 3. Click Save.

1.3.3 Establish a VPN connection

There are several ways to establish a connection.

- Right-click on the new Phase 2 in the tree control, and then click **Open Tunnel**.
- Right-click on the system tray icon, then click the name of the tunnel to open it.