

# TheGreenBow IPSec VPN Client Configuration Guide

# SonicWall TZ170

WebSite:

http://www.thegreenbow.com

Contact: <u>support@thegreenbow.com</u>

THECOECOONIA	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

# Table of contents

1	Introduction	. 3
	1.1 Goal of this document	.3
	1.2 VPN Network topology	.3
	1.3 SonicWall TZ170 VPN Gateway	.3
2	SonicWall TZ170 VPN configuration	.4
3	TheGreenBow IPSec VPN Client configuration	.4 .4 .4 .4
4	Tools in case of trouble         4.1       A good network analyser: ethereal	.4 .4
5	VPN IPSec Troubleshooting 5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) 5.2 « INVALID COOKIE » error 5.3 « no kovistato » error	.4 .4 .4
	<ul> <li>5.3 « NO Reystate » endi-</li> <li>5.4 « received remote ID other than expected » error</li></ul>	.4 .4 .4
	<ul> <li>5.6 « INVALID ID INFORMATION » error</li> <li>5.7 I clicked on "Open tunnel", but nothing happens</li></ul>	.4 .4 .4
6	Contacts	.4

THECOECOECOE 1 1010140101	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

# 1 Introduction

### 1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a SonicWall TZ170 firewall.

### 1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the SonicWall TZ170 firewall. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



### 1.3 SonicWall TZ170 VPN Gateway

The tests and VPN configuration have been conducted with a SonicWall TZ170. firmware SonicOS Standard 3.1.0.7-77s.

THECOECOEMINATION	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

# 2 SonicWall TZ170 VPN configuration

This section describes how to build an IPSec VPN configuration with your SonicWall TZ170 VPN firewall.

Once connected to your VPN gateway, you must select "**Users**" tab then "**Local User**" tabs. Click on "**Add**" for registering a new user. You can fill the following screen with your values :

TheGreenBow							
ccess (when access is restricted)							
3							
Access from VPN client with XAUTH							
TP VPN client							
ement capabilities							
OK Cancel							

When the user will connect to the gateway, he will be asked for these login and password. Click on "**Ok**" once every thing done. The new user should appear in "**Local Users**".

SONICWALL	COMPR	EHENSIVE INTER	NET SECURITY				
System Network Firewall VPN Users	Users > Local U Local Users	sers				ltems	? 1 to 1 (of 1) [3] < ▷ [3]
<ul> <li>■ Status</li> <li>■ Settings</li> <li>■ Local Users</li> </ul>	<ul> <li># Name</li> <li>1 TheGreenBow</li> <li>Add</li> </ul>	Bypass Filters No	Access to VPN No	VPN Client Yes	L2TP Client No	Limited Management No	Configure
Security Services Log Wizards Help Logout Status: Ready							

TUEGDEEDEMII 1010101	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

In the next steps, you will create an VPN tunnel with which the VPN client will be able to get connected to the SonicWall TZ170.

# Now, click on "VPN" then on "Settings".

"Enable VPN" must be checked.

SONICWALL	COMPREHENSIVE INTE	RNET SECURITY**				
System Network Firewall VPN Settings Advanced DHOP over VPN	VPN > Settings VPN Global Settings Chable VPN Unique Firewall Identifier:		VP	N Policy Wizard	Apply	Cancel ?
<ul> <li>L2TP Server</li> <li>Local Certificates</li> <li>CA Certificates</li> </ul>	VPN Policies	Gateway Ided, 3 Maximum Poli	Destinations ities Allowed	Crypto Suite ESP 3DE8 HMAC SHA	Items 1 to Enabl	1 (ort) El (L ) El e Configure
Users Security Services Log Wizards Help Logout	Currently Active VPN Tun # Name Local No Entries	inels	Remote		llems 🕛 to Gates	0 (of 0) B1 <1 ≥ B1

### In "VPN Policies", click on "Add" for adding a new VPN tunnel.

General	Proposals	Advanced	Client					
Security Policy								
IPSec Keying I	Mode:	IKE usir	ng Preshared Secret	~				
Name:		GroupVI	PN					
Shared Secret		PresharedSecret						
Ready								
			OK	Cancel	Help			

In our example, the value of the preshared key is "PresharedSecret". It must be set also on the client.

THECOECOECOE	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 - Nov.2005
	VPN version	3.0x

The proposals are the algorithms that will be used during Phase 1 and Phase 2. They will also be used in the client settings.

General	Proposals	Advanced	Client					
IKE (Phase 1) Proposal								
DH Group:		Group 2		~				
Encryption:		3DES		*				
Authentication:		SHA1		*				
Life Time (sec	onds):	28800						
Ipsec (Pha	se 2) Propo	sal						
Protocol:		ESD		~				
1 1010001.								
Encryption:		3DES		~				
Authentication:		SHA1		~				
📃 Enable Pe	rfect Forward Se	crecy						
DH Group:		Group 2	×					
Life Time (sec	onds):	28800						
Ready								
			OK	Cancel	Help			

THECOECOONHaattata	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

General	Proposals	Advanced	Client		
Advanced S	ettings				
📃 Enable Wind	Enable Windows Networking (NetBIOS) Broadcast				
📃 Apply NAT a	nd Firewall Rule	es			
📃 Forward pac	ckets to remote '	VPNs			
Default LAN Gat	eway: 0.0.0.0				
VPN Terminated	i at:				
💿 lan 🔿 oi	PT 🔿 LAN/OF	т			
Client Authe	entication				
🗹 Require Aut	hentication of VF	PN Clients via >	(AUTH		
Ready					
			OK.	Cancel	Help

General	Proposals	Advanced	Client				
User Name and Password Caching							
Cache XAUTH User Name and Password on Client: Never							
<u>Client Con</u>	nections						
Virtual Adapter	settings:		None	!		~	
Allow Connect	ions to:		All S	ecured G	ateways	~	
Set Default Route as this Gateway							
Require Global Security Client for this Connection							
Client Initial Provisioning							
Ready							
			OK		Cancel	Help	

Doc.Ref	tgbvpn_ug_TZ170_en
Doc.version	1.0 – Nov.2005
VPN version	3.0x

# 3 TheGreenBow IPSec VPN Client configuration

# 3.1 VPN Client Phase 1 (IKE) Configuration

TheGreenBow VPN Clie	ent 📃 🗖 🔀
<u>File VPN Configuration Tools</u>	2
THEGREENBOW	
	IPSec VPN Client
🚕 Console	Phase 1 (Authentication)
🍘 Parameters	Name CnxVpn1
S Connections	Interface ×
	Remote Gateway yoursonicwall.yourdomain.com
CnxVpn1	Preshared Key
	Confirm
	C Certificate Certificates Import
	IKE P1 Advanced
	Encryption 3DES
	Authentication SHA
	Key Group DH1024
	Save & Apply
VPN ready	Tunnel: 🥑

### Phase 1 configuration

In "Preshared Key"'s value textbox, you must fill the same value that was set in TZ170 configuration.

THECOECODOLIMANA	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

In phase 1 advanced settings ("P1 Advanced"), you must set "Aggressive mode" and check "X-Auth popup". In our example, the value of the "Local ID" is an IP address.

Phase1 Advanced	
	Ð
Advanced features	
🔲 Config Mode 🛛 🛛 IKE Po	t
🔽 Aggressive Mode 🛛 Redund.GW	/
X-Auth	
🔽 X-Auth Popup Logi	ו 🗌
Passwor	1
Local and Remote ID	
Choose the type of ID:	Set the value for the ID:
Remote ID	
	Ok Cancel

THECOELDOMU 1040140101	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

### 3.2 VPN Client Phase 2 (IPSec) Configuration

TheGreenBow VPN Clie	ent 🔲 🗖 🔀
File VPN Configuration Tools	?
THEGREENBOW	
	IPSec VPN Client
💫 Console	Phase 2 (IPSec Configuration)
🔯 Parameters	Name CnxVpn1
😂 Connections	VPN Client address 192 . 168 . 100 . 1
Configuration	Address type Subnet address Remote LAN address 192 . 168 . 0 . 1 Subnet Mask 255 . 255 . 0
	Encryption 3DES  P2 Advanced P2 Advanced P2 Advanced
	PFS Group None Open Tunnel
	Save & Apply
VPN ready	Tunnel: 🥑

### Phase 2 Configuration

In "VPN Client address", you may define a static virtual IP address.

If you use 0.0.0.0, you will have error "Local-ID" is missing. It does not prevent you from establishing a tunnel

### 3.3 Open IPSec VPN tunnels

Once both SonicWall TZ170 firewall and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on "Save & Apply" to take into account all modifications we have made on your VPN Client configuration

2. Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)

3. Select "Connections" to see opened VPN Tunnels

4. Select "Console" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging.

THECOECOECOE	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

# 4 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

### 4.1 A good network analyser: ethereal

Ethereal is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website <u>http://www.ethereal.com/</u>. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.

THECPEEDEMI MO140101	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

## 5 VPN IPSec Troubleshooting

### 5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [NOTIFY] 114920 Default exchange\_run: exchange\_validate failed 114920 Default dropped message from 195.100.205.114 port 500 due to notification type PAYLOAD\_MALFORMED 114920 Default SEND Informational [NOTIFY] with PAYDAD\_MALFORMED error

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

### 5.2 « INVALID COOKIE » error

115933 Default message\_recv: invalid cookie(s) 59Bca0c2634288f 7364e3e486e49105 115933 Default dropped message from 195.100.205.114 port 500 due to notification type INVALID\_COOKIE 115933 Default SEND Informational [NOTIFY] with INVALID\_COOKIE error

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN connection on each side.

### 5.3 « no keystate » error

115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID] 115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE] 115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE] 115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY] 115319 Default ipsec\_get\_keystate: no keystate in SAKMP SA 00B57C50

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

### 5.4 « received remote ID other than expected » error

120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID] 120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE] 120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default ike\_phase\_1\_recv\_ID: received remote ID other than expected support@thegreenbow.fr

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

THECOECOECOE	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

### 5.5 « NO PROPOSAL CHOSEN » error

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID] 115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE] 115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE] 115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY] 115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114 115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Ouick Mode [SA][KEY][ID][HASH][NONCE] 115915 Default RECV Informational [HASH][NOTIFY] with NO\_PROPOSAL\_CHOSEN error 115915 Default RECV Informational [HASH][DEL] 115915 Default CNXVPN1-P1 deleted

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 115911 Default RECV Informational [NOTIFY] with NO\_PROPOSAL<u>C</u>HOSEN error

### 5.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID]
122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
                          CNXVPN1-CNXVPN1-P2)
                                                        phase
122626
         Default
                   (SA
                                                 SEND
                                                                      Ouick
                                                                               Mode
                                                                  2
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

If you have an «INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4\_ADDR type (and not a IPV4\_SUBNET type).

### 5.7 I clicked on "Open tunnel", but nothing happens.

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

### 5.8 The VPN tunnel is up but I can't ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- ? Check Phase 2 settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- ? Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall. Check that every device between the client and the VPN server does accept ESP
- ? Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- ? Check your ISP supports ESP

THECOECOECIE	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

- ? If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal for example). You will have an indication that encryption works.
- ? Check the "default gateway" value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no "Default gateway" setting.
- ? You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN except if you set "DNS server" and "WINS server" in "P2 Advanced" windows from the client interface.
- ? We recommend you to install ethereal (http://www.ethereal.com) on one of your target computer. You can check that your pings arrive inside the LAN.

THEGREERBOW	Doc.Ref	tgbvpn_ug_TZ170_en
	Doc.version	1.0 – Nov.2005
	VPN version	3.0x

# 6 Contacts

News and updates on TheGreenBow web site : <u>http://www.thegreenbow.com</u> Technical support by email at <u>support@thegreenbow.com</u> Sales contacts at +33 1 43 12 39 37 ou by email at <u>info@thegreenbow.com</u>