TheGreenBow IPSec VPN Client

Configuration Guide

Zywall 5

WebSite:	http://www.thegreenbow.com
Contact:	support@thegreenbow.com

Table of contents

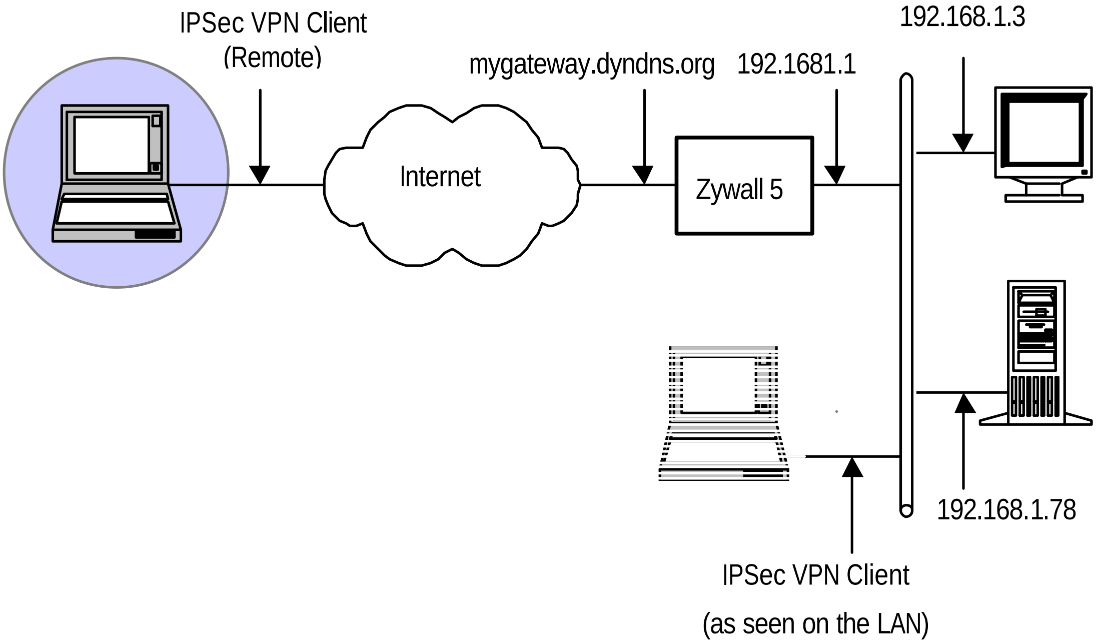
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Zywall 5 VPN router.

1.2 VPN Network topology

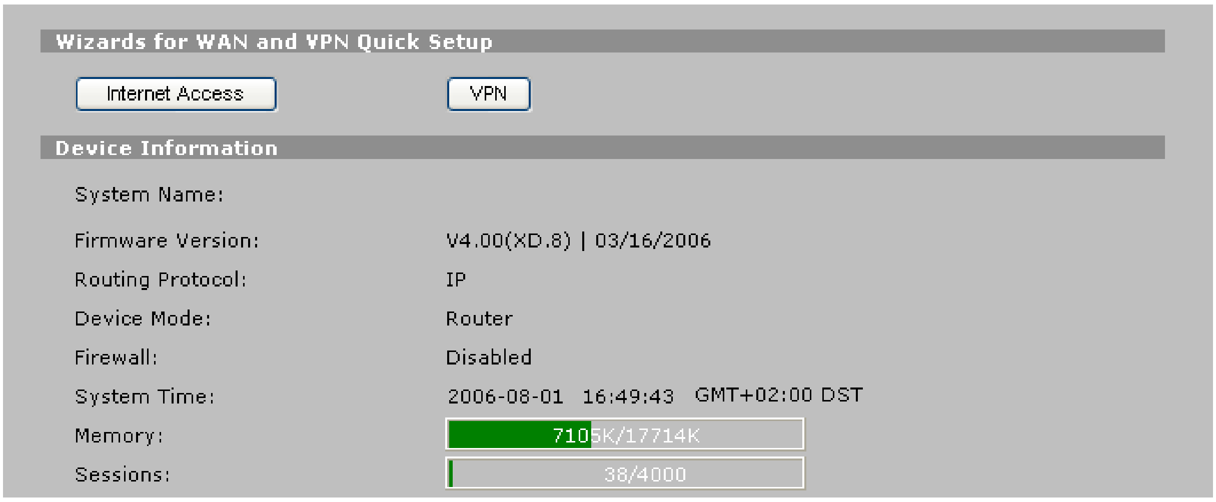
In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the Zywall 5 router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



2 Zywall 5 VPN configuration

This section describes how to build an IPSec VPN configuration with your Zywall 5 VPN router.

In this section, the VPN wizard will be used. It is available from the "HOME" web interface.

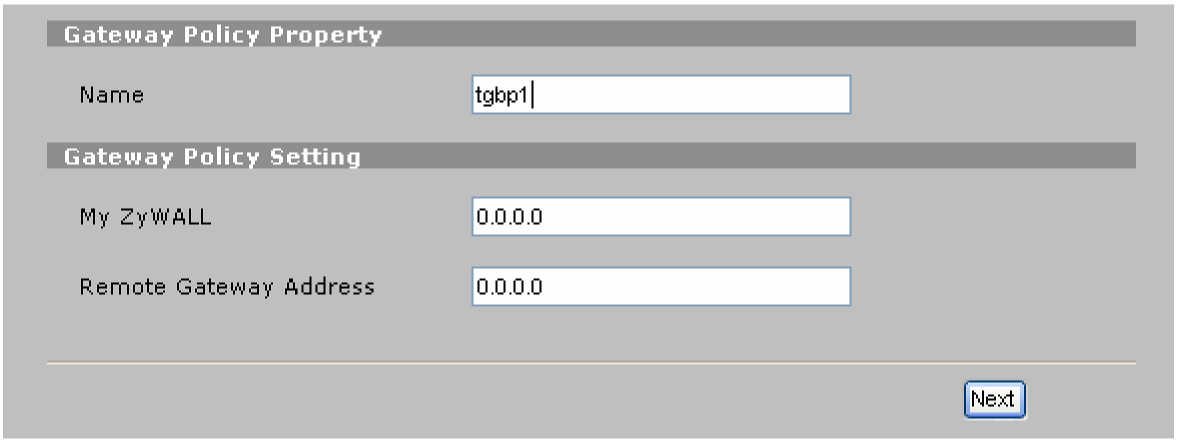


Wizards for WAN and VPN Quick Setup

Device Information

System Name:	
Firmware Version:	V4.00(XD.8) | 03/16/2006
Routing Protocol:	IP
Device Mode:	Router
Firewall:	Disabled
System Time:	2006-08-01 16:49:43 GMT+02:00 DST
Memory:	7105K/17714K
Sessions:	38/4000

Click on "VPN".



Gateway Policy Property

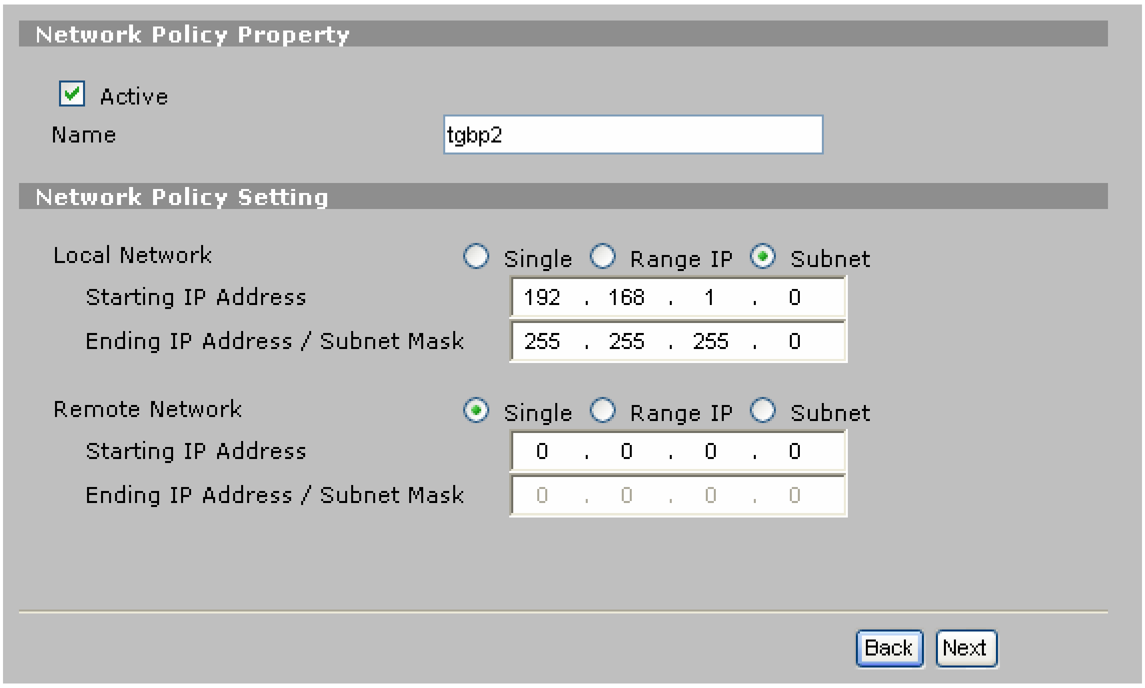
Name: tgbp1

Gateway Policy Setting

My ZyWALL: 0.0.0.0

Remote Gateway Address: 0.0.0.0

The first screen configures some P1 settings. Click on "Next".



Network Policy Property

☑ Active

Name: tgbp2

Network Policy Setting

Local Network: ○ Single ○ Range IP ● Subnet

Starting IP Address: 192 . 168 . 1 . 0

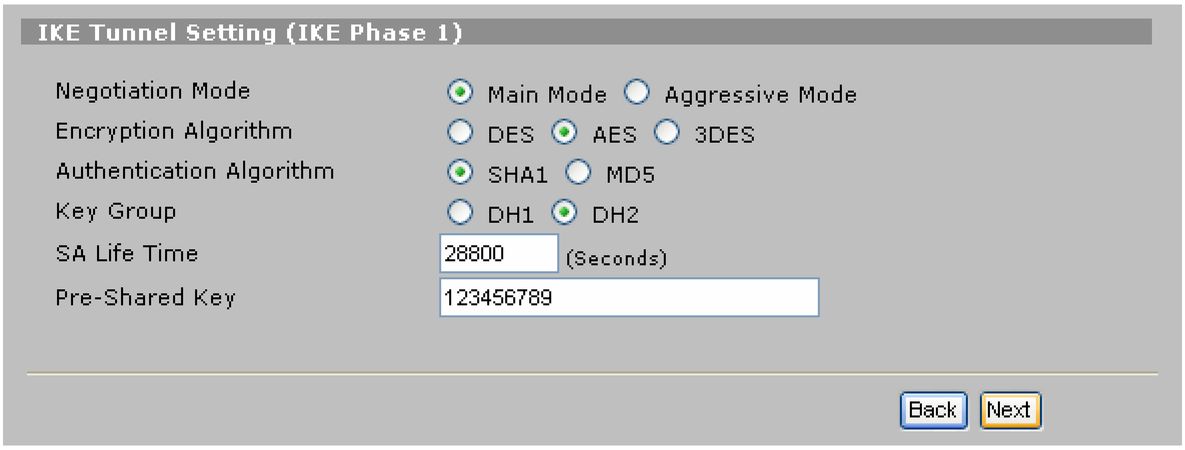
Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Remote Network: ● Single ○ Range IP ○ Subnet

Starting IP Address: 0 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 0 . 0 . 0 . 0

The second screen configures Phase 2 identities. Click on “Next”.



IKE Tunnel Setting (IKE Phase 1)

Negotiation Mode: ● Main Mode ○ Aggressive Mode

Encryption Algorithm: ○ DES ● AES ○ 3DES

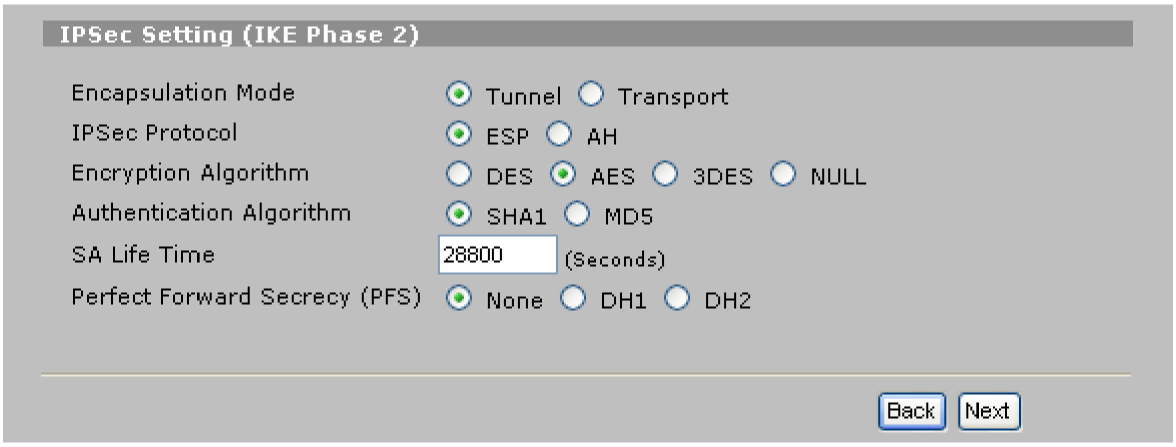
Authentication Algorithm: ● SHA1 ○ MD5

Key Group: ○ DH1 ● DH2

SA Life Time: 28800 (Seconds)

Pre-Shared Key: 123456789

The third screen configures the phase 1 algorithms and the preshared key. Click on “Next”



IPSec Setting (IKE Phase 2)

Encapsulation Mode: ● Tunnel ○ Transport

IPSec Protocol: ● ESP ○ AH

Encryption Algorithm: ○ DES ● AES ○ 3DES ○ NULL

Authentication Algorithm: ● SHA1 ○ MD5

SA Life Time: 28800 (Seconds)

Perfect Forward Secrecy (PFS): ● None ○ DH1 ○ DH2

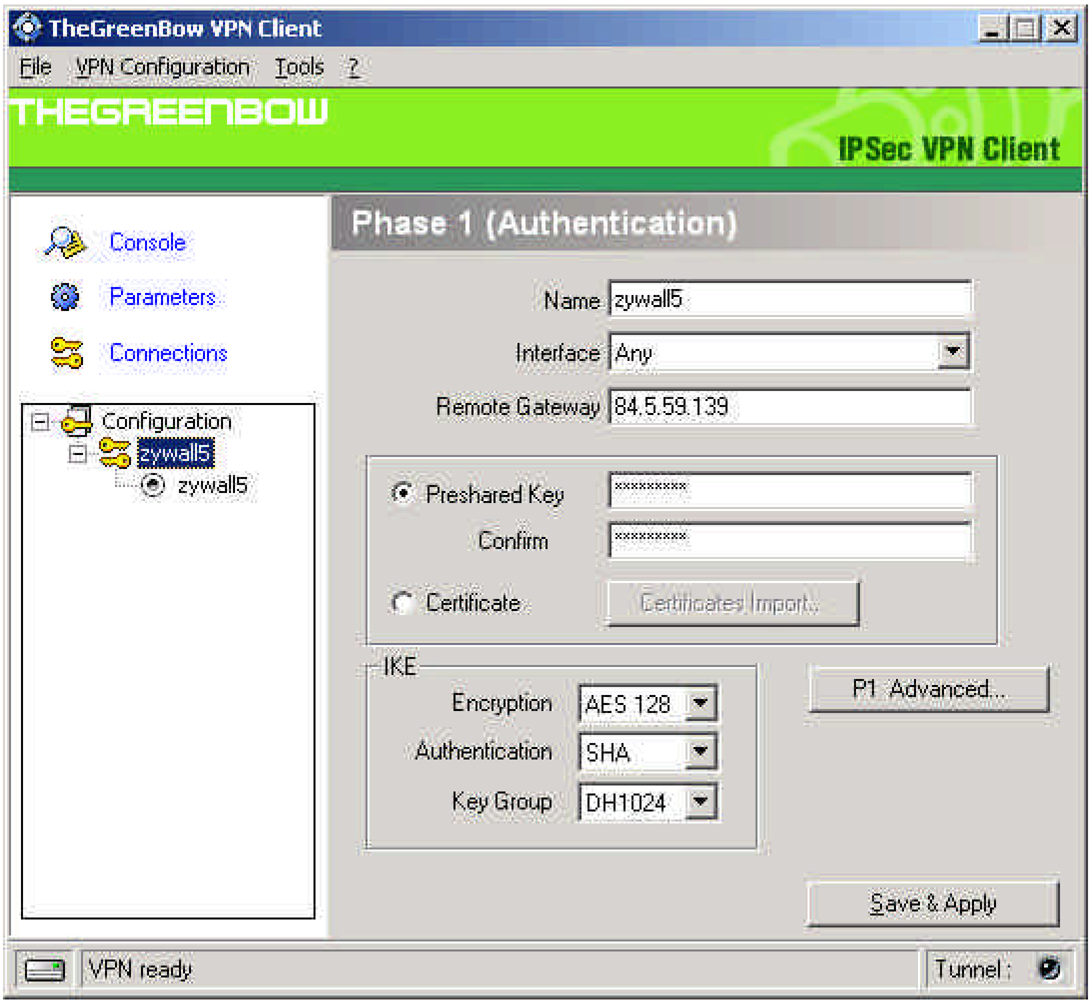
The fourth and last screen configures the phase 2 algorithms. Click on “Next” and on “Finish”.

Write down these settings. They will be used in TheGreenBow VPN client. This tunnel can be used with several TheGreenBow IPSec clients.

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

Right-click on "Configuration" and create a phase 1. Fill field in the same way than the screenshot below.



Phase 1 (Authentication)

Name: zywall5

Interface: Any

Remote Gateway: 84.5.59.139

● Preshared Key: *********

Confirm: *********

○ Certificate

IKE

Encryption: AES 128

Authentication: SHA

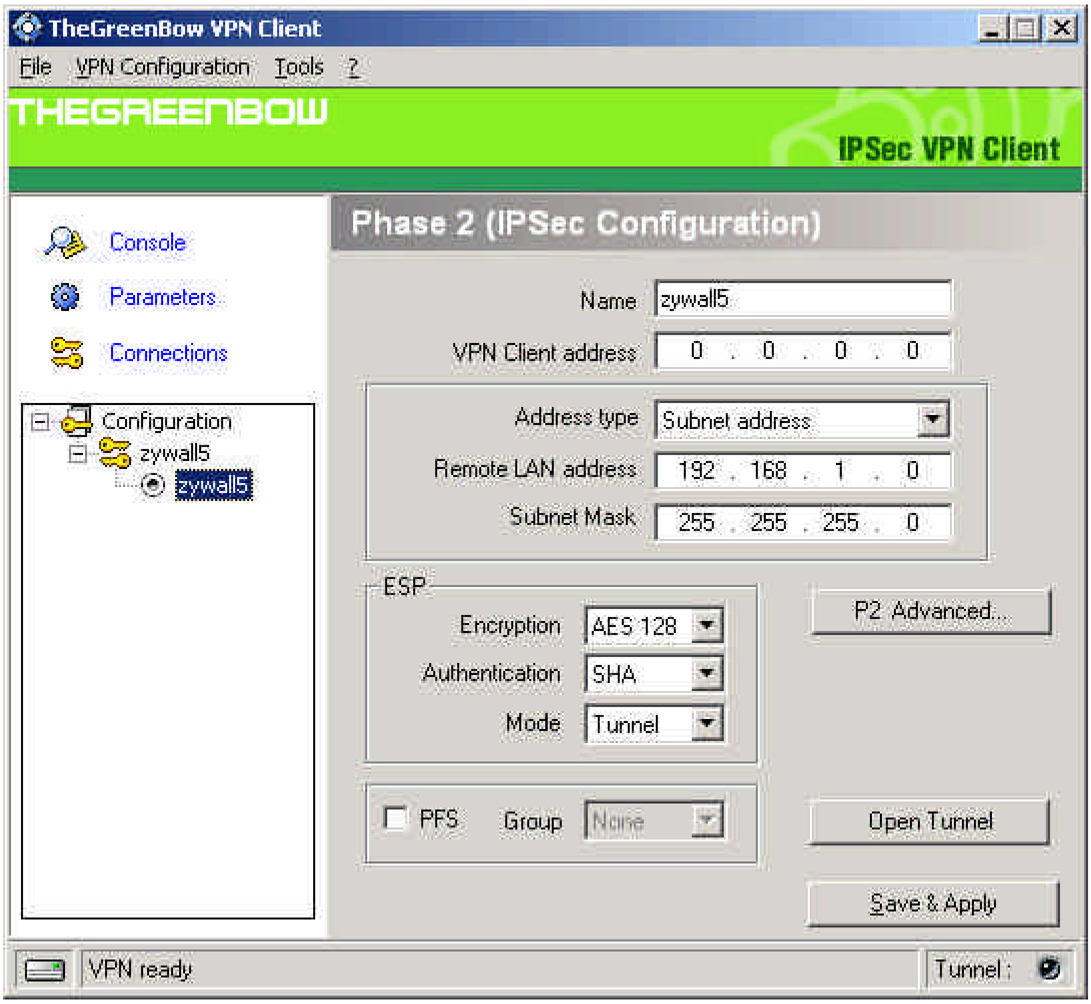
Key Group: DH1024

Phase 1 configu ration

No configuration is needed in "P1 advanced".

3.2 VPN Client Phase 2 (IPSec) Configuration

Right-click on Phase 1 and create a Phase 2.



Phase 2 (IPSec Configuration)

Name: zywall5

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: AES 128

Authentication: SHA

Mode: Tunnel

□ PFS Group: None

Phase 2 Configuration

VPN client address can be let to 0.0.0.0. In that case, the VPN client will used local computer IP address.

3.3 Open IPSec VPN tunnels

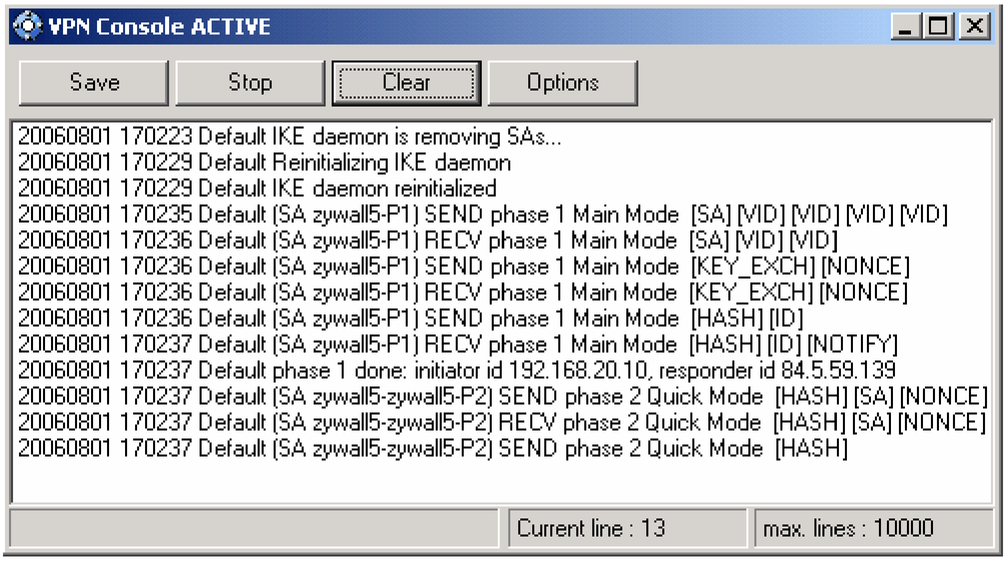
Once both Zywall 5 router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

1. Click on "**Save & Apply**" to take into account all modifications we've 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**". A successful connection should look like the next screenshot:



```
20060801 170223 Default IKE daemon is removing SAs...
20060801 170229 Default Reinitializing IKE daemon
20060801 170229 Default IKE daemon reinitialized
20060801 170235 Default (SA zywall5-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID]
20060801 170236 Default (SA zywall5-P1) RECV phase 1 Main Mode  [SA] [VID] [VID]
20060801 170236 Default (SA zywall5-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE]
20060801 170236 Default (SA zywall5-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE]
20060801 170236 Default (SA zywall5-P1) SEND phase 1 Main Mode  [HASH] [ID]
20060801 170237 Default (SA zywall5-P1) RECV phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20060801 170237 Default phase 1 done: initiator id 192.168.20.10, responder id 84.5.59.139
20060801 170237 Default (SA zywall5-zywall5-P2) SEND phase 2 Quick Mode  [HASH] [SA] [NONCE]
20060801 170237 Default (SA zywall5-zywall5-P2) RECV phase 2 Quick Mode  [HASH] [SA] [NONCE]
20060801 170237 Default (SA zywall5-zywall5-P2) SEND phase 2 Quick Mode  [HASH]
```

Current line : 13

max. lines : 10000

4 VPN IPSec Troubleshooting

4.1 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.

4.1.1 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 tools is available on website http://www.ethereal.com/. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.

4.1.2 Network Scanner

Network Scanner from Softperfect can be used for checking that the remote network is available. It can be downloaded from http://www.softperfect.com/products/networkscanner/

4.2 « 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 PAYLOAD_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.

4.3 « INVALID COOKIE » error

```
115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 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.

4.4 « 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 ISAKMP 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.

4.5 « 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  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.

4.6 « 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    Quick    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_CHOSEN error
```

4.7 « 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
122626    Default    (SA    CNXVPN1-CNXVPN1-P2)    SEND    phase    2    Quick    Mode
[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).

4.8 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).

4.9 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

? 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.

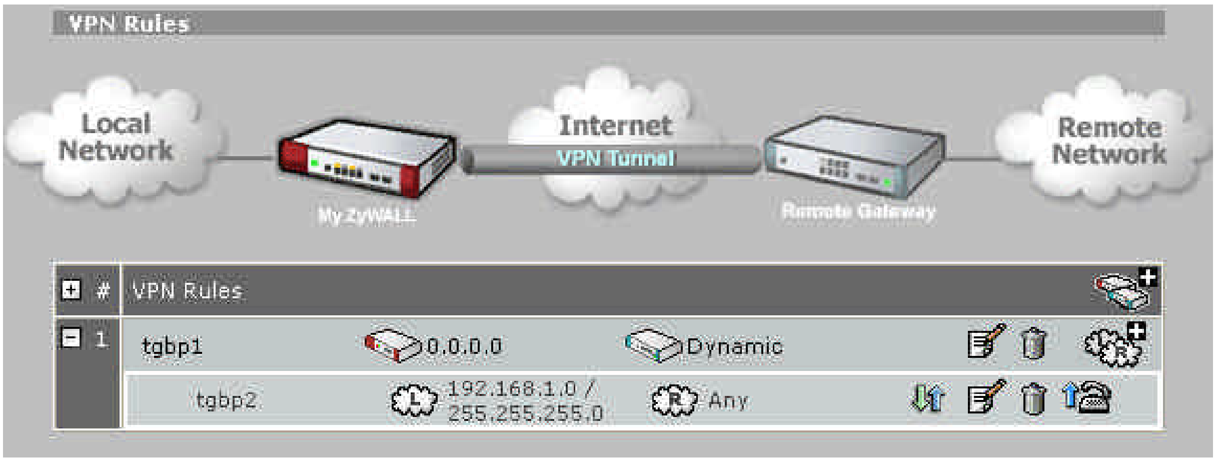
? You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.

? 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.

5 X-Auth configuration

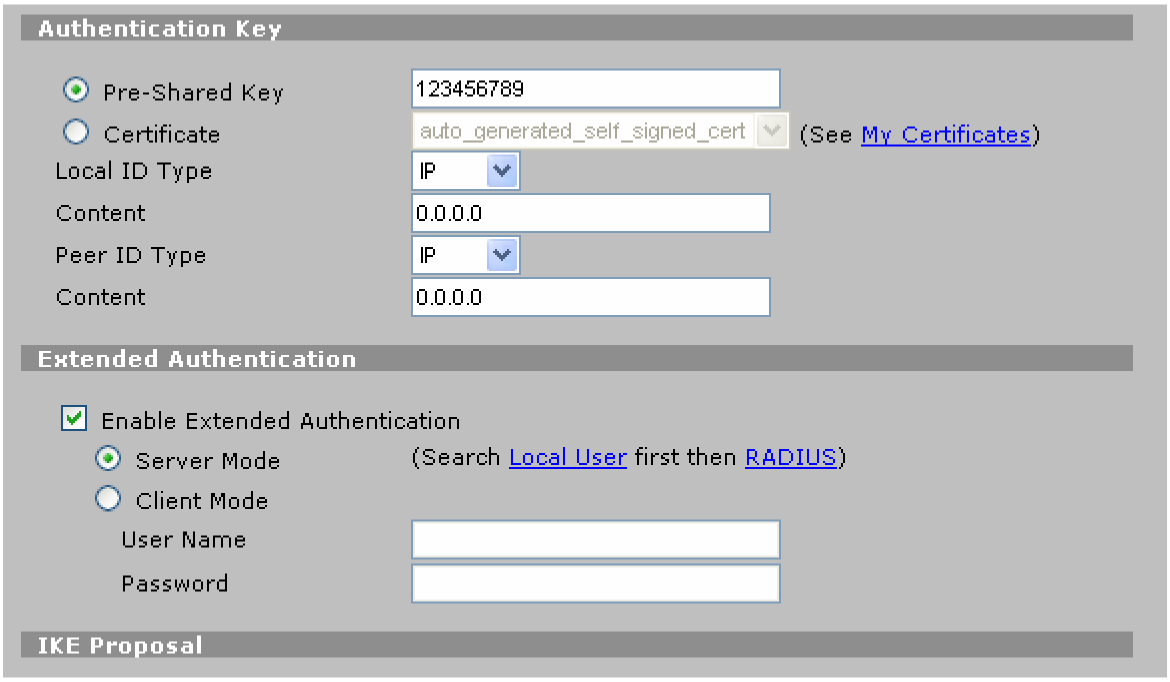
The Zywall 5 offers functionalities that increase security for roadwarrior connection. One of them is X-Auth authentication. IT managers can add a user to a database and give access to him/her with a password. When the user leaves the company, its setting is remove and he/she cannot connect any more.

In the main interface, click on “Security” and on “VPN” when all the connections available can be found :



#	VPN Rules			
1	tgbp1	0.0.0.0	Dynamic	
	tgbp2	192.168.1.0 / 255.255.255.0	Any	

Edit phase 1 settings by clicking on 📝.



Authentication Key

● Pre-Shared Key	123456789
○ Certificate	auto_generated_self_signed_cert (See My Certificates)
Local ID Type	IP
Content	0.0.0.0
Peer ID Type	IP
Content	0.0.0.0

Extended Authentication

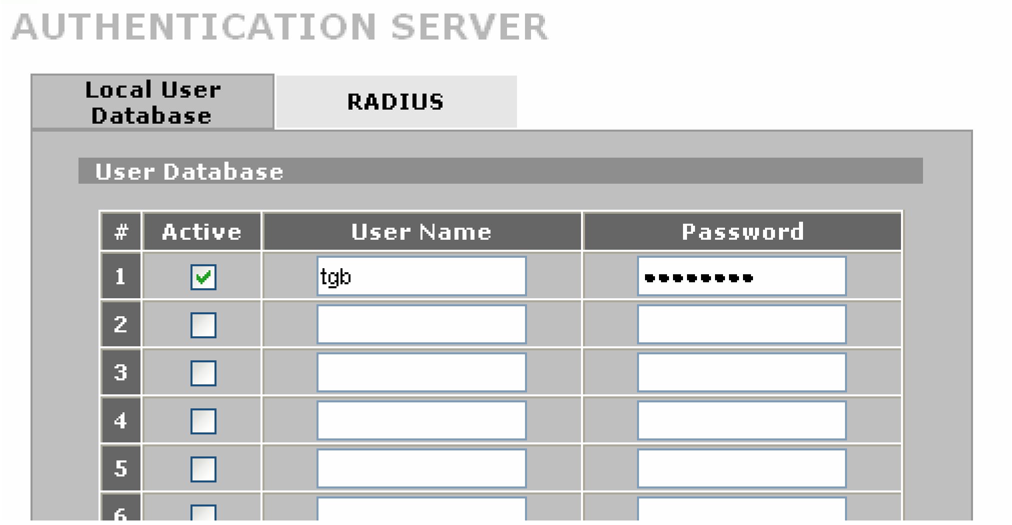
☑ Enable Extended Authentication

● Server Mode	(Search Local User first then RADIUS)
○ Client Mode	
User Name	
Password	

IKE Proposal

Select “Enable Extended Authentication” and “Server Mode” and click on “Apply”.

Click then on “Security” and “Auth Server”.



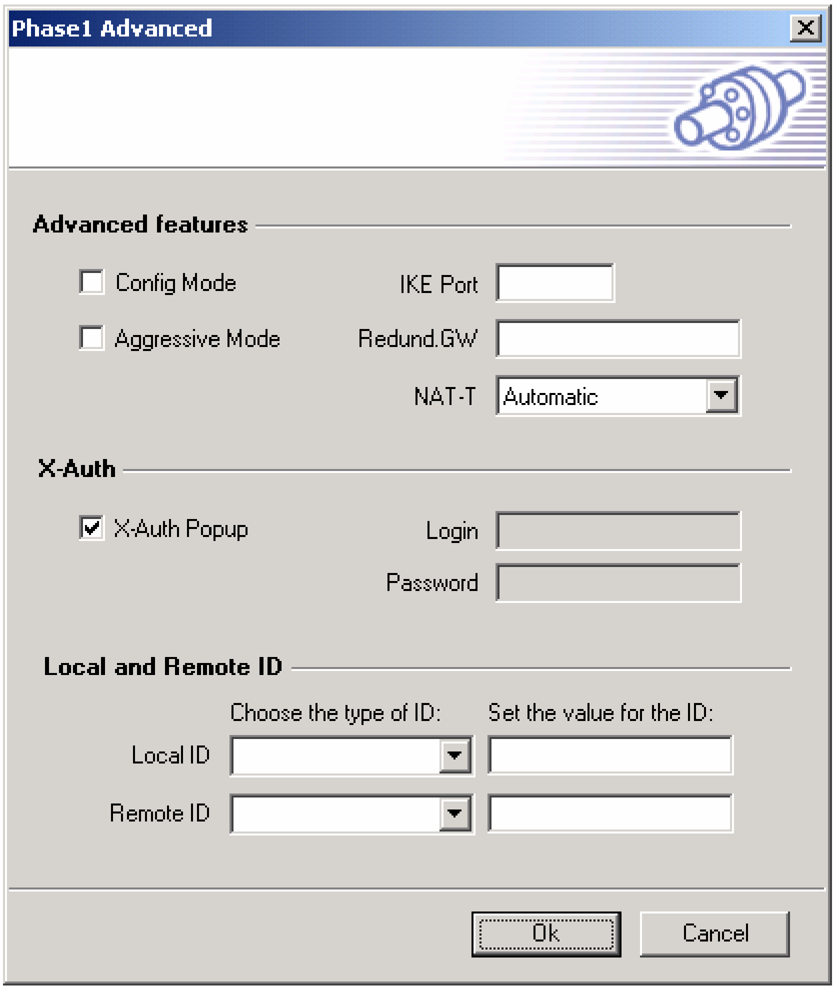
AUTHENTICATION SERVER

User Database

#	Active	User Name	Password
1	☑	tgb	●●●●●●●●●
2	□		
3	□		
4	□		
5	□		
6	□		

In "Local User Database", " add an user name and a password. Click on "Apply".

On TheGreenBow IPSec client, select the phase 1 and click on "P1 Advanced… ".



Phase1 Advanced

Advanced features

- □ Config Mode
- □ Aggressive Mode
- IKE Port:
- Redund.GW:
- NAT-T: Automatic

X-Auth

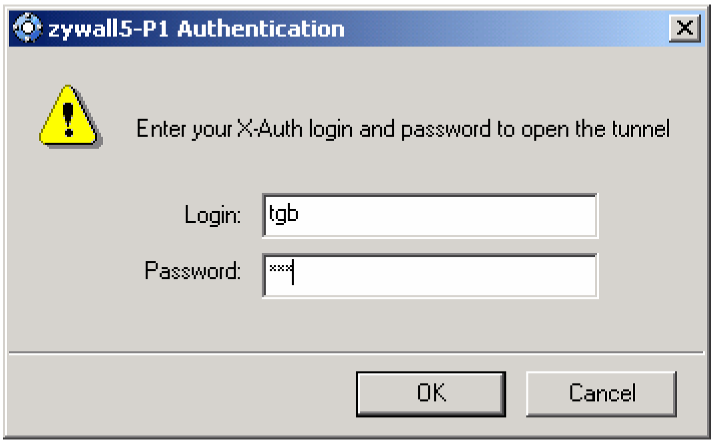
- ☑ X-Auth Popup
- Login:
- Password:

Local and Remote ID

	Choose the type of ID:	Set the value for the ID:
Local ID		
Remote ID		

Check "X-Auth Popup" if you do not want the login/password to be stored in the configuration file and click on "OK".

When the user opens the tunnel a popup appears :



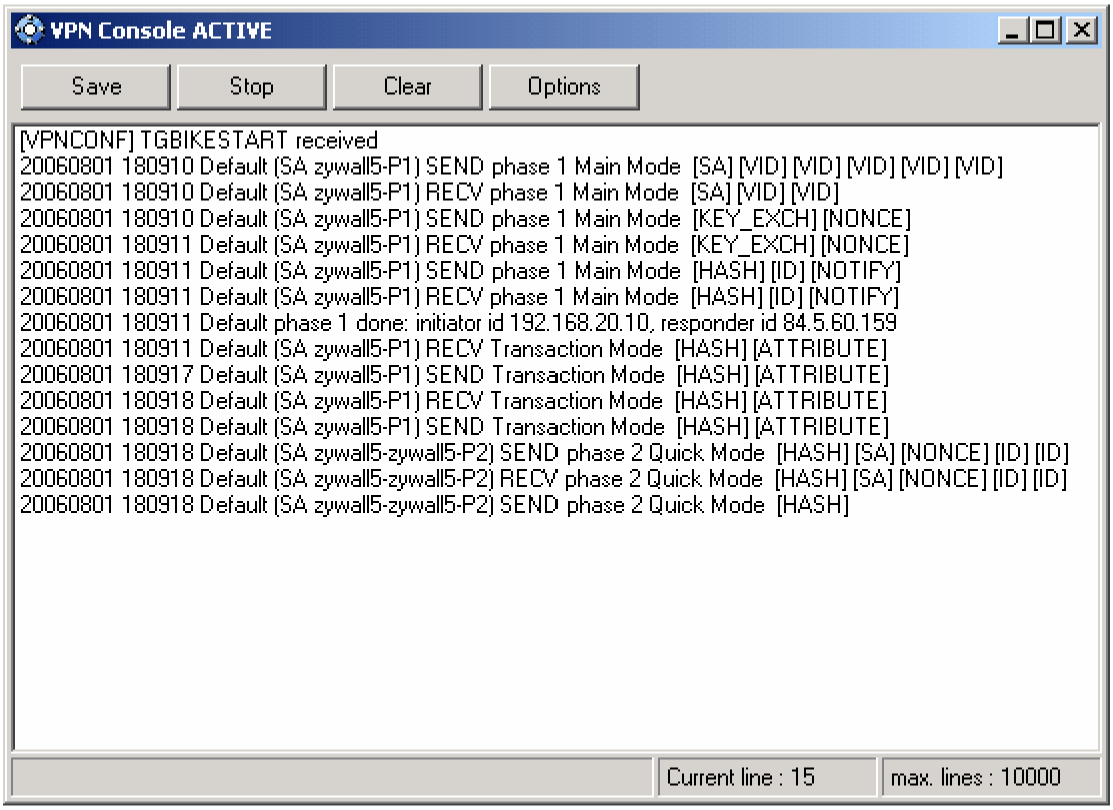
zywall5-P1 Authentication

Enter your X-Auth login and password to open the tunnel

Login: tgb

Password: ***

If the credentials are correct the tunnel is established. Logs in the console should look like this :



VPN Console ACTIVE

```
[VPNCONF] TGBIKESTART received
20060801 180910 Default (SA zywall5-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID] [VID]
20060801 180910 Default (SA zywall5-P1) RECV phase 1 Main Mode  [SA] [VID] [VID]
20060801 180910 Default (SA zywall5-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE]
20060801 180911 Default (SA zywall5-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE]
20060801 180911 Default (SA zywall5-P1) SEND phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20060801 180911 Default (SA zywall5-P1) RECV phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20060801 180911 Default phase 1 done: initiator id 192.168.20.10, responder id 84.5.60.159
20060801 180911 Default (SA zywall5-P1) RECV Transaction Mode  [HASH] [ATTRIBUTE]
20060801 180917 Default (SA zywall5-P1) SEND Transaction Mode  [HASH] [ATTRIBUTE]
20060801 180918 Default (SA zywall5-P1) RECV Transaction Mode  [HASH] [ATTRIBUTE]
20060801 180918 Default (SA zywall5-P1) SEND Transaction Mode  [HASH] [ATTRIBUTE]
20060801 180918 Default (SA zywall5-zywall5-P2) SEND phase 2 Quick Mode  [HASH] [SA] [NONCE] [ID] [ID]
20060801 180918 Default (SA zywall5-zywall5-P2) RECV phase 2 Quick Mode  [HASH] [SA] [NONCE] [ID] [ID]
20060801 180918 Default (SA zywall5-zywall5-P2) SEND phase 2 Quick Mode  [HASH]
```

Current line : 15 | max. lines : 10000

6 Contacts

News and updates on TheGreenBow web site : http://www.thegreenbow.com

Technical support by email at support@thegreenbow.com

Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com