TheGreenBow IPSec VPN Client

Configuration Guide

ZyXEL ZyWALL P1 firmware V3.64

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 ZyXEL ZyWALL P1 with firmware 3.64

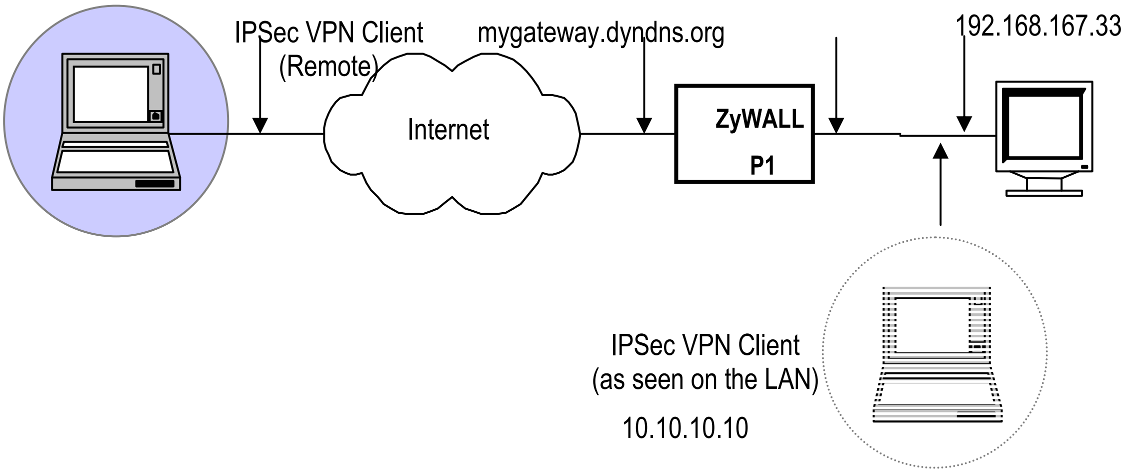
1.2 VPN Network topology

This gateway is a personal firewall with very limited LAN capabilities (DHCP for a single IP address for example).

Eventhough Zyxel highlights its nomad VPN client features (which connects to a VPN server), it can also be configured as a VPN server usable with a road warrior vpn client like TheGreenBow. In this case both server and client can be nomads.

It can also be configured with a NAT device behind it, hidding a LAN overriding its limited LAN features, but this is not the purpose of this document.

External IP of the ZyWALL P1:	mygateway.dyndns.org (or public IP address)
IP Subnet behind the ZyWALL P1:	192.168.167.0/255.255.255.0



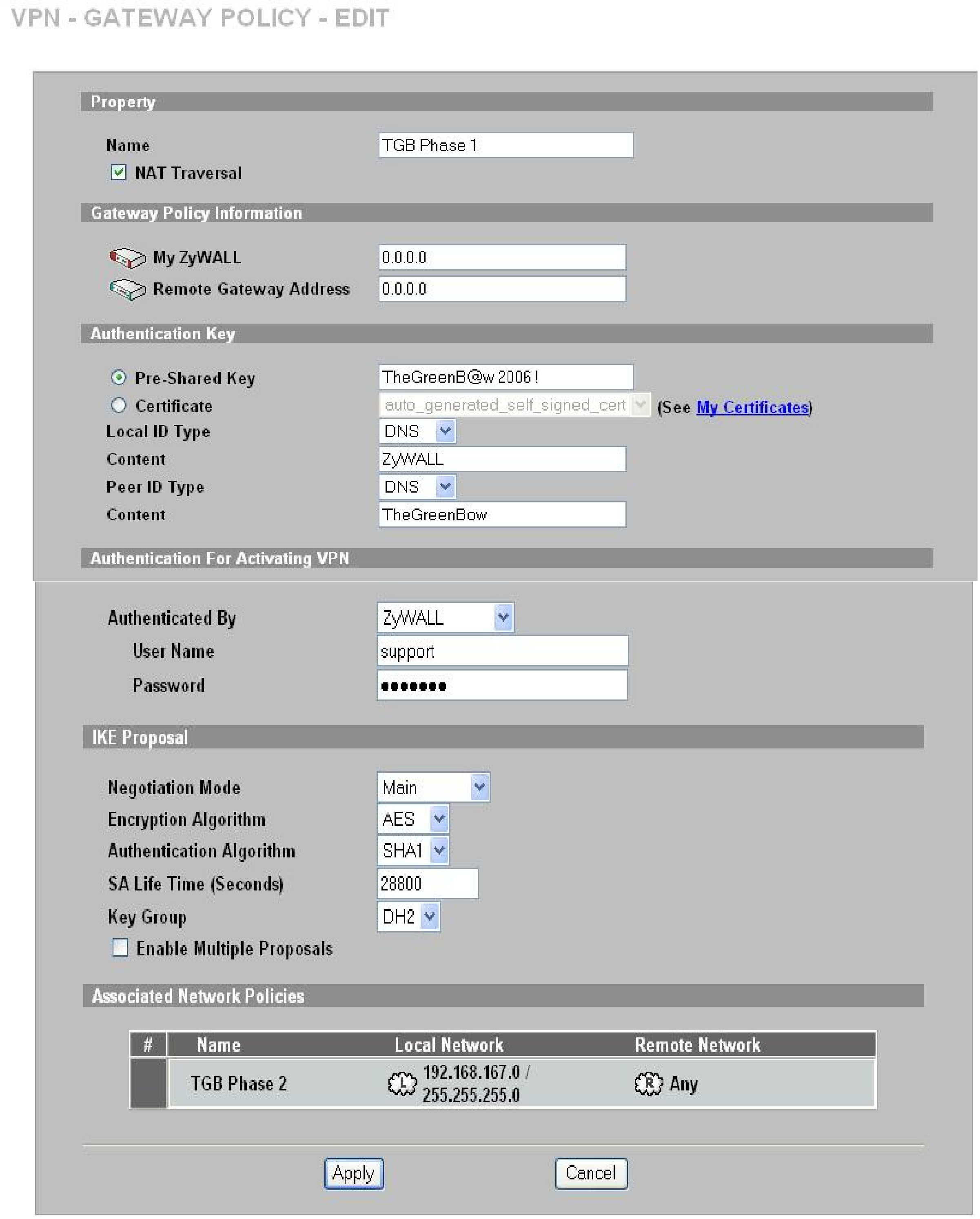
2 Setup ZyWALL P1

This section describes how to build an IPSec VPN configuration with ZyWALL P1 VPN Gateway.

There is no mandatory configuration, all settings may be altered to match your needs (speed vs security)

2.1 Gateway Policy

Create a new gateway policy on the ZyWALL (related to phase 1 on TheGreenBow VPN Client):



VPN - GATEWAY POLICY - EDIT

Property

Name: TGB Phase 1

☑ NAT Traversal

Gateway Policy Information

My ZyWALL: 0.0.0.0

Remote Gateway Address: 0.0.0.0

Authentication Key

● Pre-Shared Key: TheGreenB@w 2006 !

○ Certificate: auto_generated_self_signed_cert (See My Certificates)

Local ID Type: DNS

Content: ZyWALL

Peer ID Type: DNS

Content: TheGreenBow

Authentication For Activating VPN

Authenticated By: ZyWALL

User Name: support

Password: •••••••

IKE Proposal

Negotiation Mode: Main

Encryption Algorithm: AES

Authentication Algorithm: SHA1

SA Life Time (Seconds): 28800

Key Group: DH2

☐ Enable Multiple Proposals

Associated Network Policies

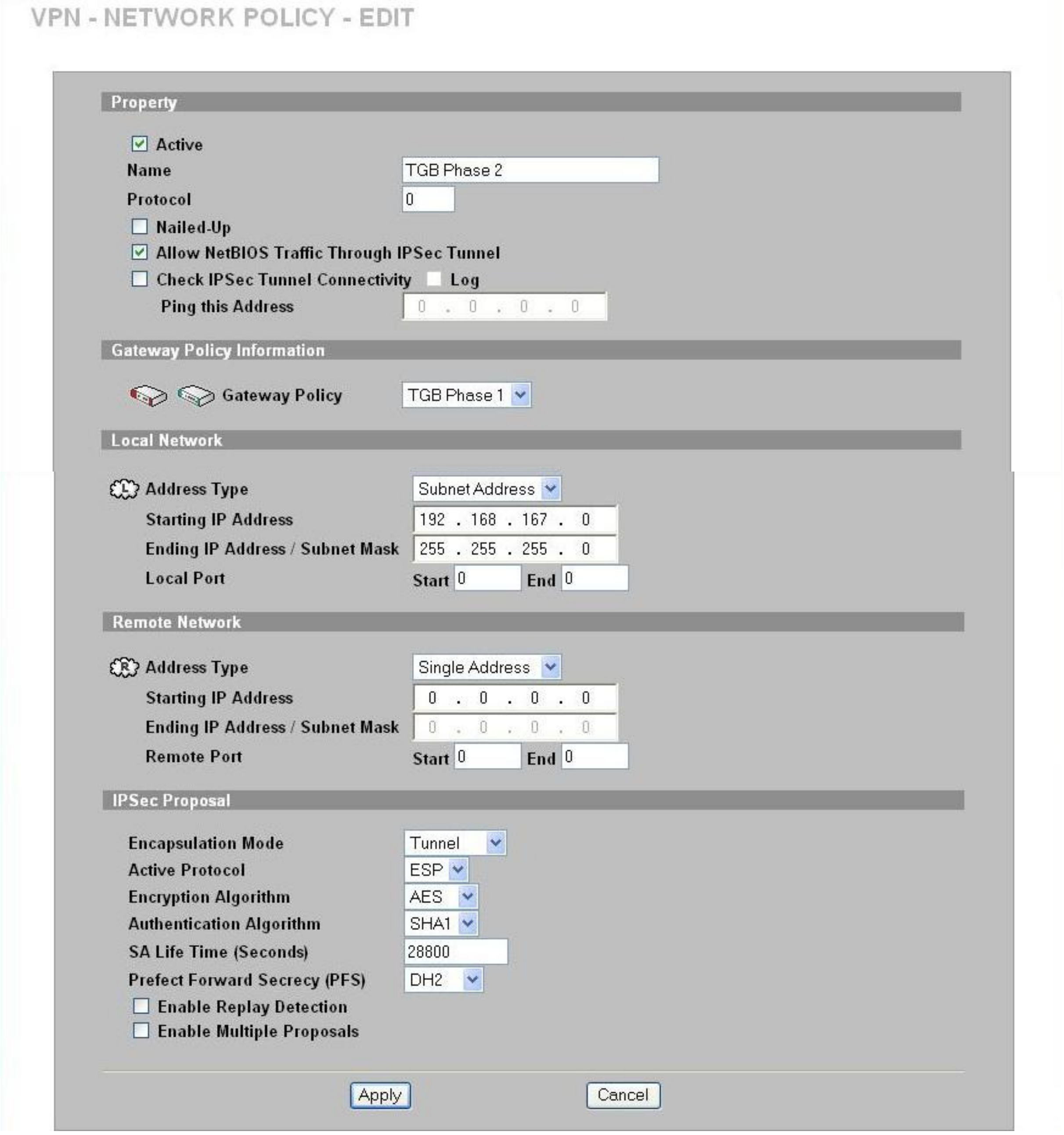
#	Name	Local Network	Remote Network
	TGB Phase 2	192.168.167.0 / 255.255.255.0	Any

We used “Main mode” instead of “Aggressive mode” because of the lack of security with “Aggressive” compared to “Main”

AES algorithm is more efficient than DES or 3DES (faster to cipher data and more secured), but anything can be used.

2.2 Network Policy

Create a new Network policy (related to phase 2 on TheGreenBow VPN client)



VPN - NETWORK POLICY - EDIT

Property

☑ Active

Name: TGB Phase 2

Protocol: 0

☐ Nailed-Up

☑ Allow NetBIOS Traffic Through IPSec Tunnel

☐ Check IPSec Tunnel Connectivity ☐ Log

Ping this Address: 0 . 0 . 0 . 0

Gateway Policy Information

Gateway Policy: TGB Phase 1

Local Network

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 167 . 0

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

Local Port: Start 0 End 0

Remote Network

Address Type: Single Address

Starting IP Address: 0 . 0 . 0 . 0

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

Remote Port: Start 0 End 0

IPSec Proposal

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: AES

Authentication Algorithm: SHA1

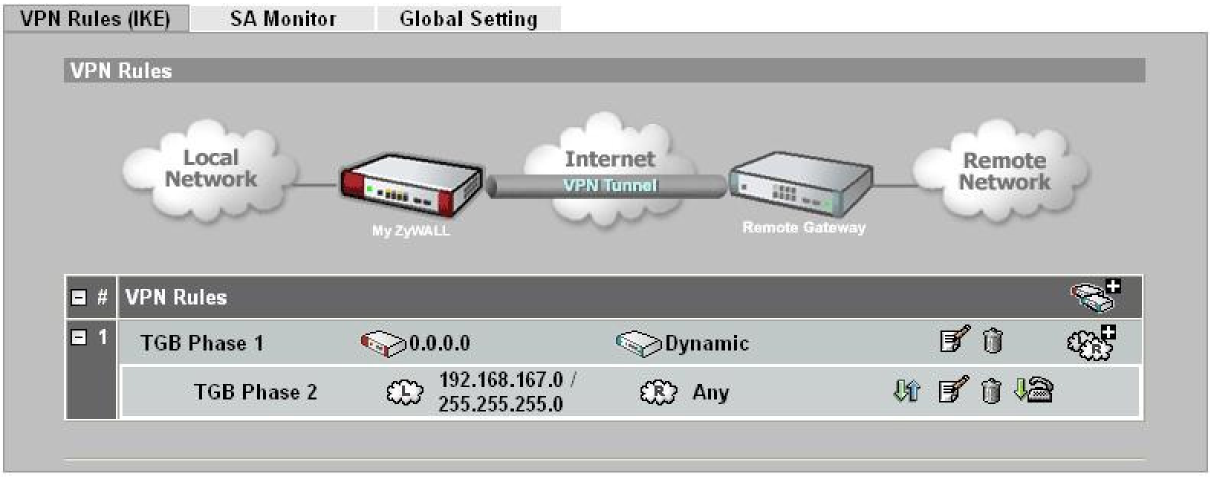
SA Life Time (Seconds): 28800

Prefect Forward Secrecy (PFS): DH2

☐ Enable Replay Detection

☐ Enable Multiple Proposals

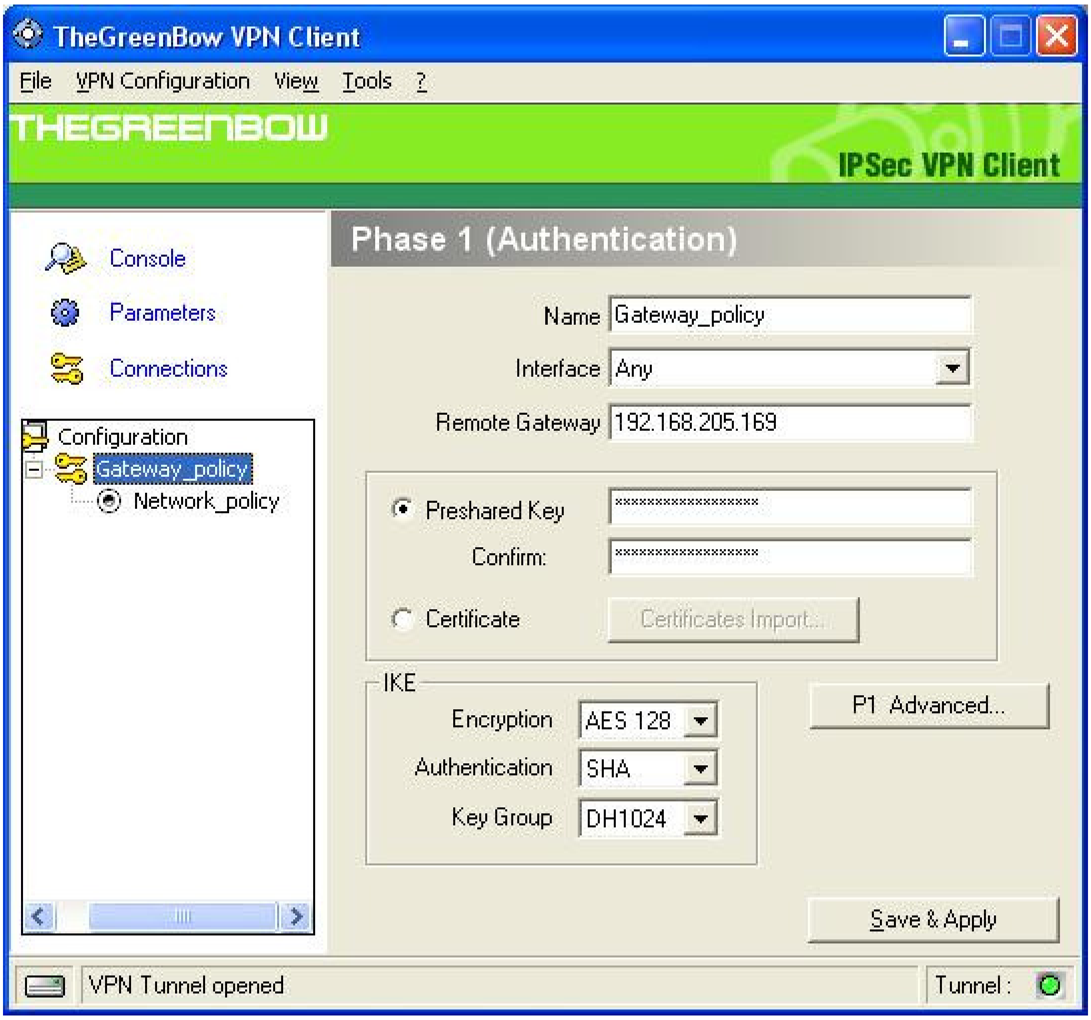
2.3 VPN configuration overview



#	VPN Rules		
1	TGB Phase 1	0.0.0.0	Dynamic
	TGB Phase 2	192.168.167.0 / 255.255.255.0	Any

3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 Configuration



Phase 1 (Authentication)

Name: Gateway_policy

Interface: Any

Remote Gateway: 192.168.205.169

● Preshared Key: ********************

Confirm: ********************

○ Certificate

IKE

Encryption: AES 128

Authentication: SHA

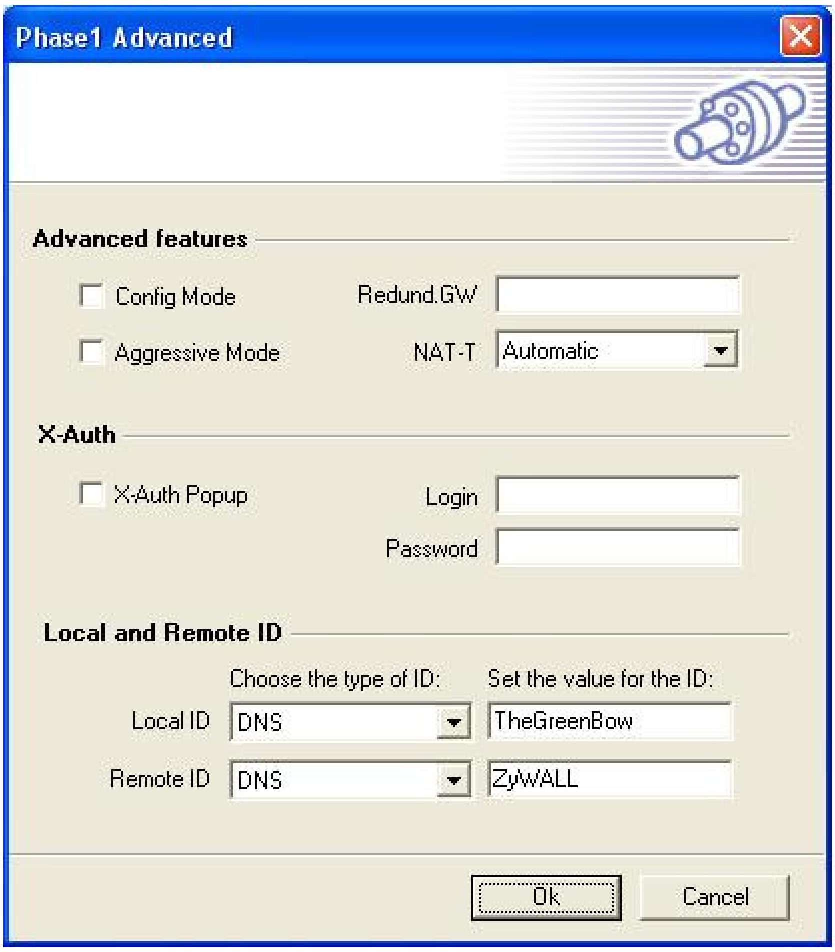
Key Group: DH1024

VPN Tunnel opened

Tunnel : ●

You MUST change “Remote Gateway” IP address to match your dyndns name or static public ip address.

Click on “P1 Advanced…” to setup IDs.



Phase1 Advanced

Advanced features

□ Config Mode

Redund.GW

□ Aggressive Mode

NAT-T: Automatic

X-Auth

□ X-Auth Popup

Login

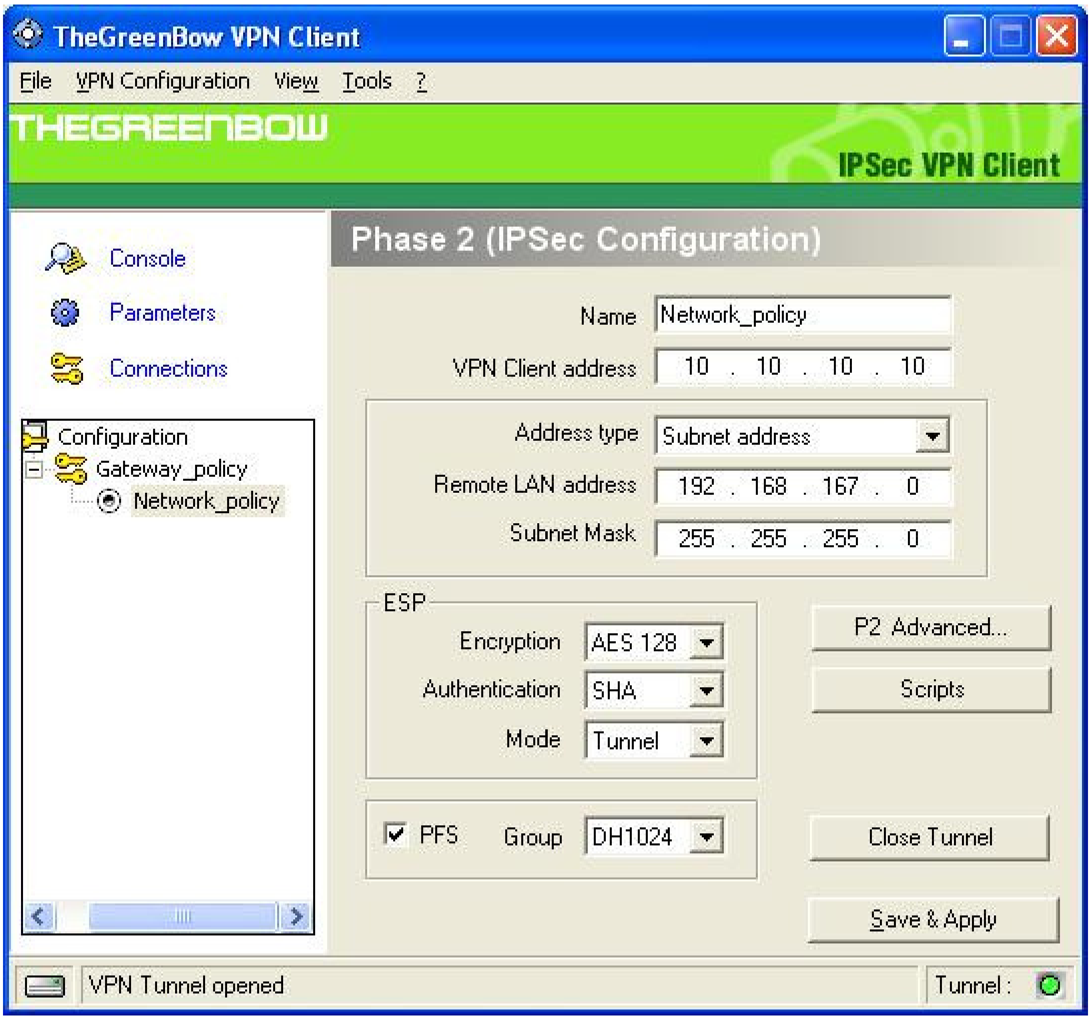
Password

Local and Remote ID

	Choose the type of ID:	Set the value for the ID:
Local ID	DNS	TheGreenBow
Remote ID	DNS	ZyWALL

ID used in this example are DNS type. These type and values must match between vpn client and router even though they are just flags that can contain any value (in the example, the values entered are NOT proper dns names, but match between client and router)

3.2 VPN Client Phase 2 Configuration



Phase 2 (IPSec Configuration)

Name: Network_policy

VPN Client address: 10 . 10 . 10 . 10

Address type: Subnet address

Remote LAN address: 192 . 168 . 167 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: AES 128

Authentication: SHA

Mode: Tunnel

☑ PFS Group: DH1024

VPN Tunnel opened

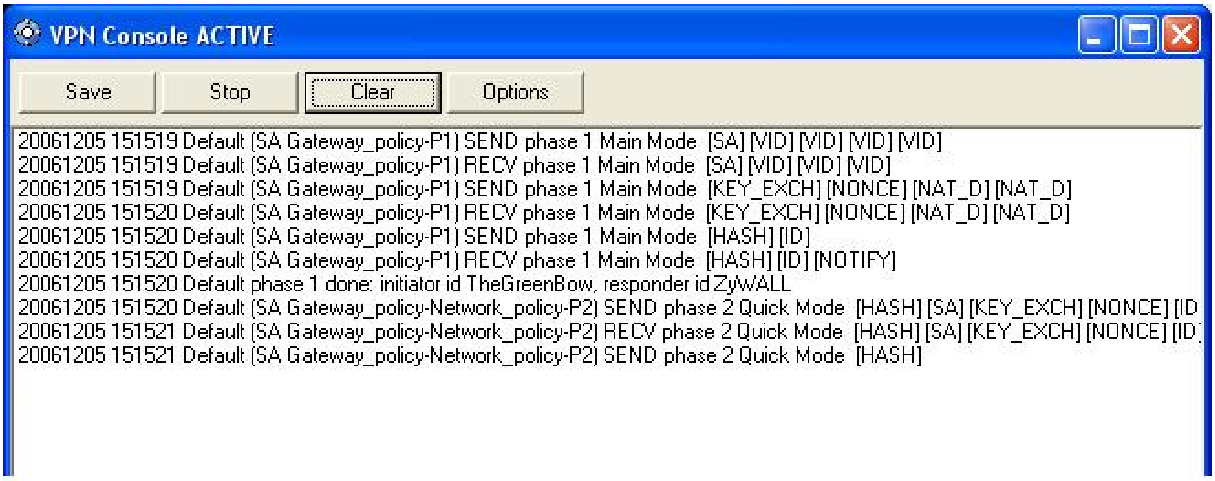
Tunnel : ●

The VPN client address must not belong to the remote subnet range (virtual IP address 10.10.10.10).

Phase2 advanced is used to enter alternate dns and/or wins servers addresses from the ones the vpn client is using prior to establish the tunnel.

3.3 Console log

The console screenshot below, shows a successful vpn connection with the P1.



```
20061205 151519 Default (SA Gateway_policy-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID]
20061205 151519 Default (SA Gateway_policy-P1) RECV phase 1 Main Mode  [SA] [VID] [VID] [VID]
20061205 151519 Default (SA Gateway_policy-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20061205 151520 Default (SA Gateway_policy-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20061205 151520 Default (SA Gateway_policy-P1) SEND phase 1 Main Mode  [HASH] [ID]
20061205 151520 Default (SA Gateway_policy-P1) RECV phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20061205 151520 Default phase 1 done: initiator id TheGreenBow, responder id ZyWALL
20061205 151520 Default (SA Gateway_policy-Network_policy-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID
20061205 151521 Default (SA Gateway_policy-Network_policy-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID
20061205 151521 Default (SA Gateway_policy-Network_policy-P2) SEND phase 2 Quick Mode  [HASH]
```

4 VPN IPSec Troubleshooting

4.1 « PAYLOAD MALFORMED » error

```
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.

4.2 « 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.

4.3 « 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 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.

4.4 « 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 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.

4.5 « 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   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
```

4.6 « 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
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).

4.7 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, UDP port 4500 and protocol ESP (protocol 50).

4.8 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 support 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 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