TheGreenBow IPSec VPN Client

Configuration Guide

Zywall 10

WebSite: http://www.thegreenbow.com

Contact: support@thegreenbow.com

Table of contents

1 Introduction 3
1.1 Goal of this document 3
1.2 VPN Network topology 3
1.3 Zyxel Zywall 10 Restrictions 3
1.4 Zyxel Zywall 10 VPN Gateway 3
1.5 Zyxel Zywall 10 VPN Gateway product info 3
2 Zyxel Zywall 10 VPN configuration 4
3 TheGreenBow IPSec VPN Client configuration 8
3.1 VPN Client Phase 1 (IKE) Configuration 8
3.2 VPN Client Phase 2 (IPSec) Configuration 10
3.3 Open IPSec VPN tunnels 10
4 Tools in case of trouble 12
4.1 A good network analyser: Wireshark 12
5 VPN IPSec Troubleshooting 13
5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA]) 13
5.2 « INVALID COOKIE » error 13
5.3 « no keystate » error 13
5.4 « received remote ID other than expected » error 13
5.5 « NO PROPOSAL CHOSEN » error 14
5.6 « INVALID ID INFORMATION » error 14
5.7 I clicked on “Open tunnel”, but nothing happens. 14
5.8 The VPN tunnel is up but I can’t ping ! 14
6 Contacts 16

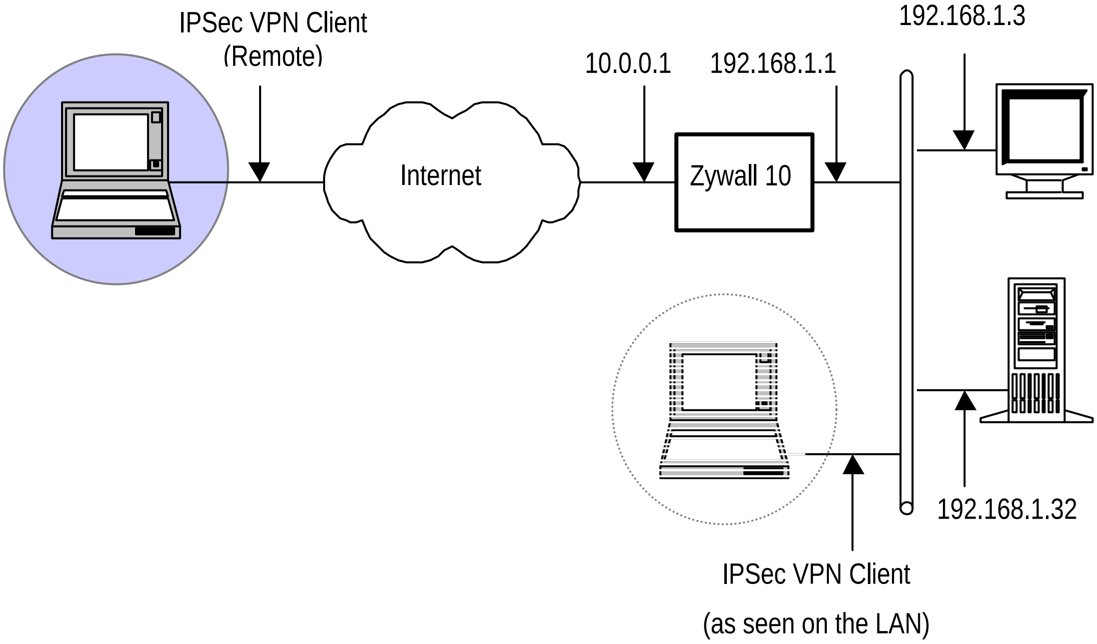
1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Zyxel Zywall 10 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 Zyxel Zywall 10 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.



1.3 Zyxel Zywall 10 Restrictions

No known restriction.

1.4 Zyxel Zywall 10 VPN Gateway

Our tests and VPN configuration have been conducted with Zyxel Zywall 10 release 3.52.

1.5 Zyxel Zywall 10 VPN Gateway product info

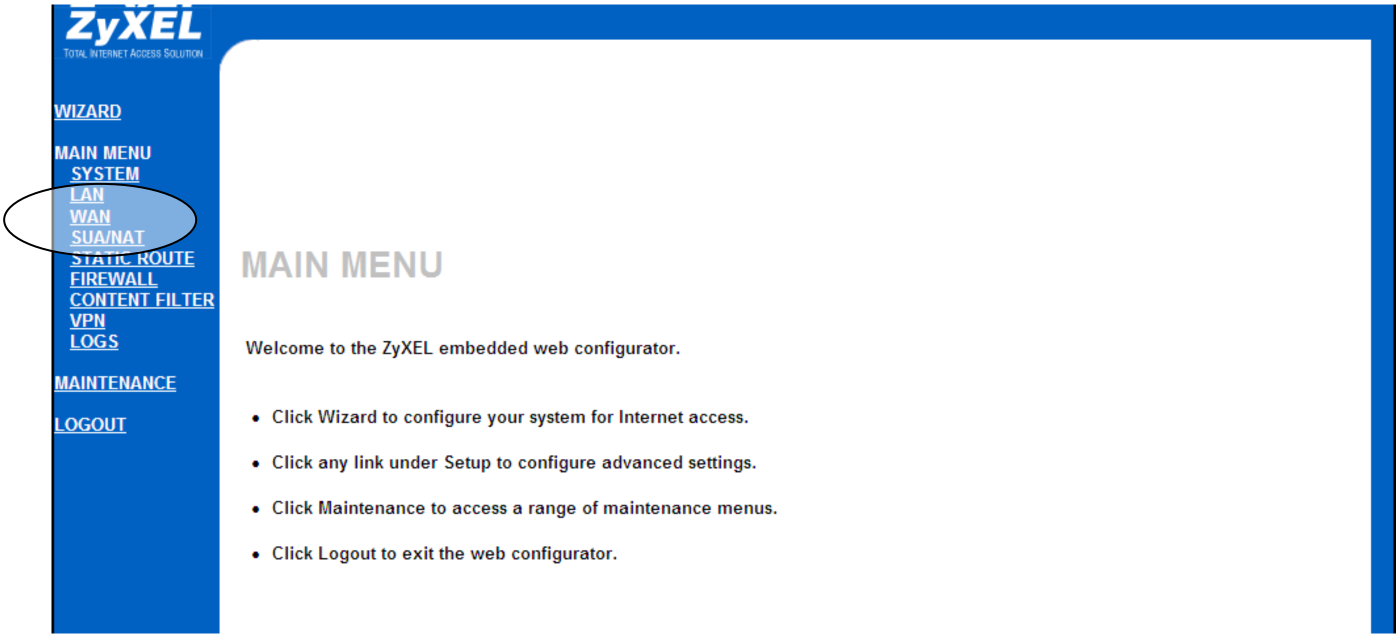
It is critical that users find all necessary information about Zyxel Zywall 10 VPN Gateway. All product info, User Guide and knowledge base for the Zyxel Zywall 10 VPN Gateway can be found on the Zywall 10 website: www.zyxel.com.

- Zywall Product page: http://us.zyxel.com/products/category.php?indexFlagvalue=1021873683

2 Zyxel Zywall 10 VPN configuration

This section describes how to build an IPSec VPN configuration with your Zywall 10 VPN router.

Once connected to your Zywall 10 VPN gateway, the home page will show Main Menu.

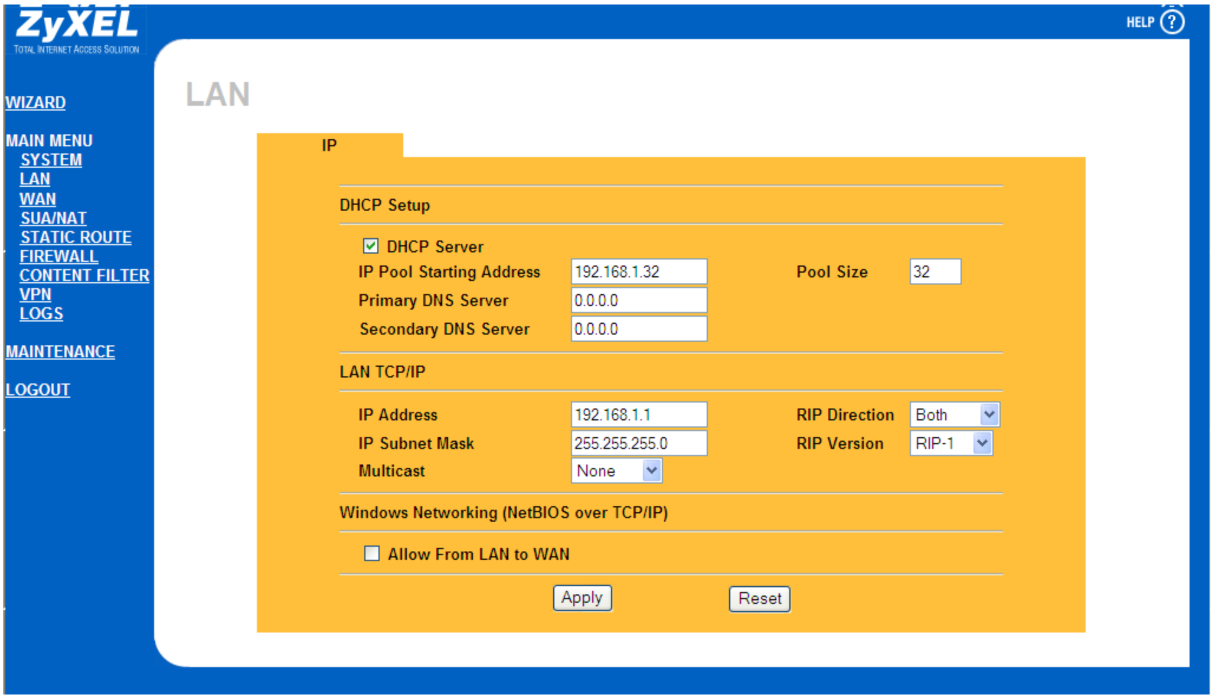


MAIN MENU

Welcome to the ZyXEL embedded web configurator.

- Click Wizard to configure your system for Internet access.
- Click any link under Setup to configure advanced settings.
- Click Maintenance to access a range of maintenance menus.
- Click Logout to exit the web configurator.

So first step is to configure the LAN.



LAN

DHCP Setup

☑ DHCP Server

IP Pool Starting Address: 192.168.1.32 — Pool Size: 32

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

LAN TCP/IP

IP Address: 192.168.1.1 — RIP Direction: Both

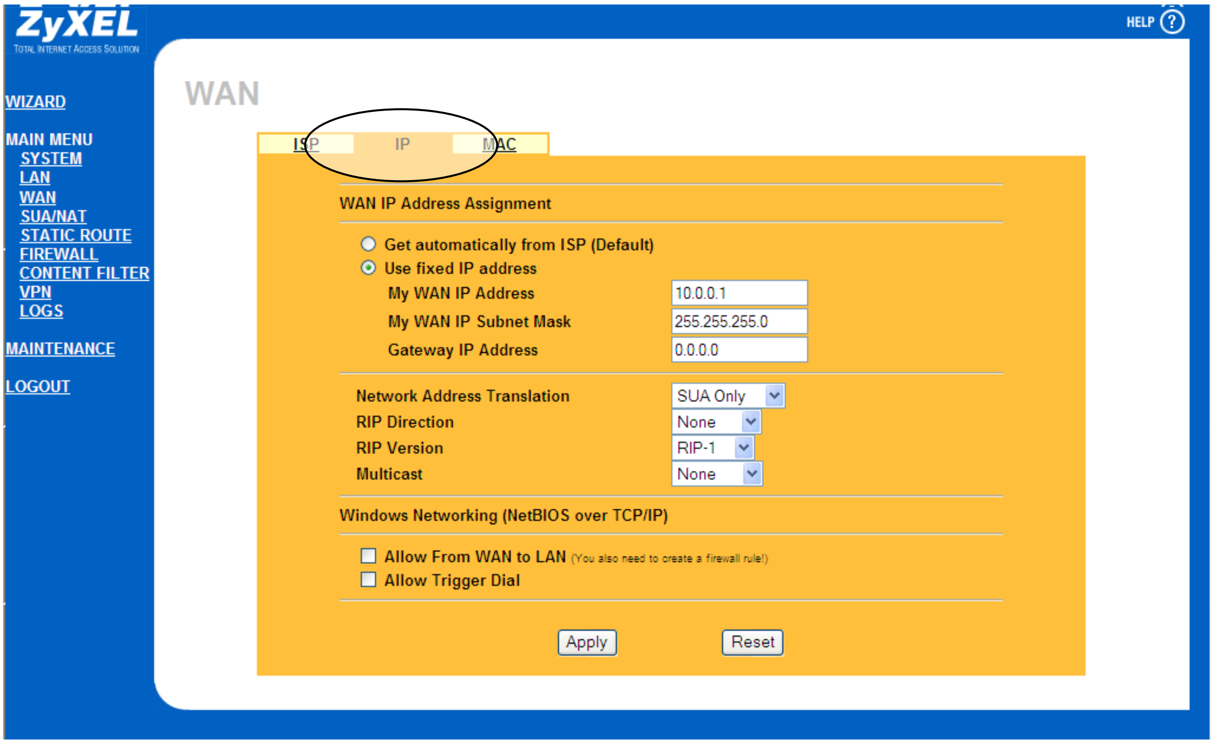
IP Subnet Mask: 255.255.255.0 — RIP Version: RIP-1

Multicast: None

Windows Networking (NetBIOS over TCP/IP)

☐ Allow From LAN to WAN

Then in the 'WAN' section, you click on 'IP': don't forget to take note of this WAN IP address as it will be used as the remote gateway address in TheGreenBow IPSec VPN Client



WAN

WAN IP Address Assignment

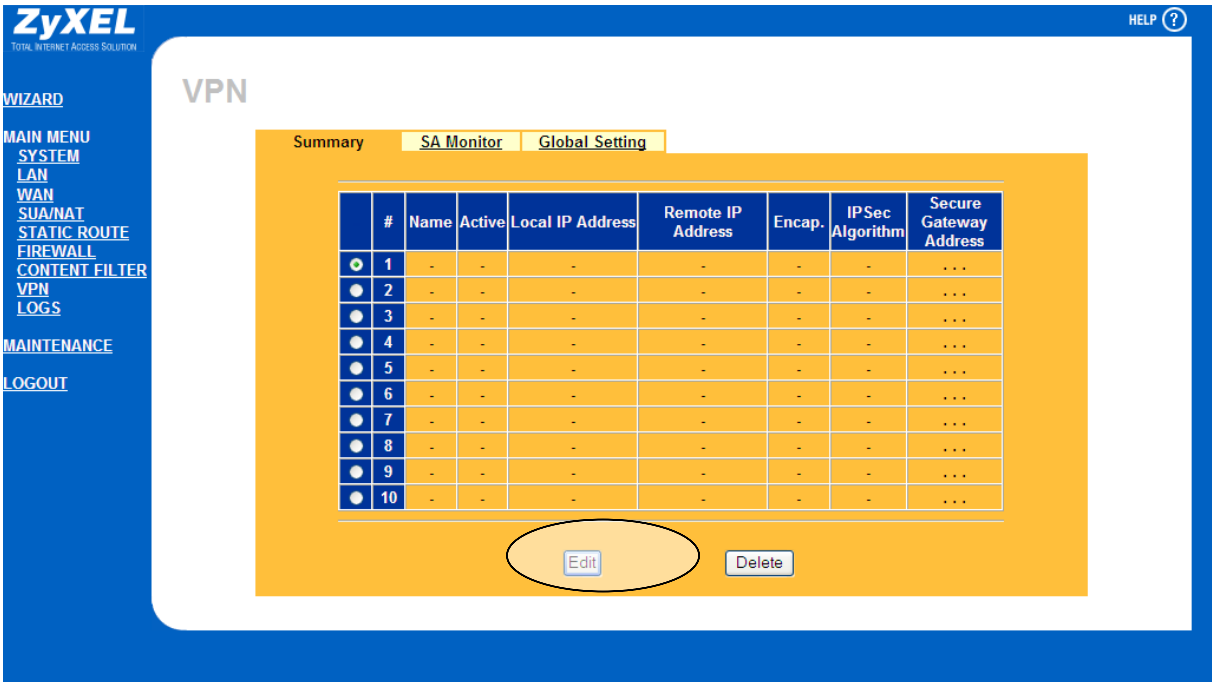
○ Get automatically from ISP (Default)
● Use fixed IP address

My WAN IP Address	10.0.0.1
My WAN IP Subnet Mask	255.255.255.0
Gateway IP Address	0.0.0.0
Network Address Translation	SUA Only
RIP Direction	None
RIP Version	RIP-1
Multicast	None

Windows Networking (NetBIOS over TCP/IP)

□ Allow From WAN to LAN (You also need to create a firewall rule!)
□ Allow Trigger Dial

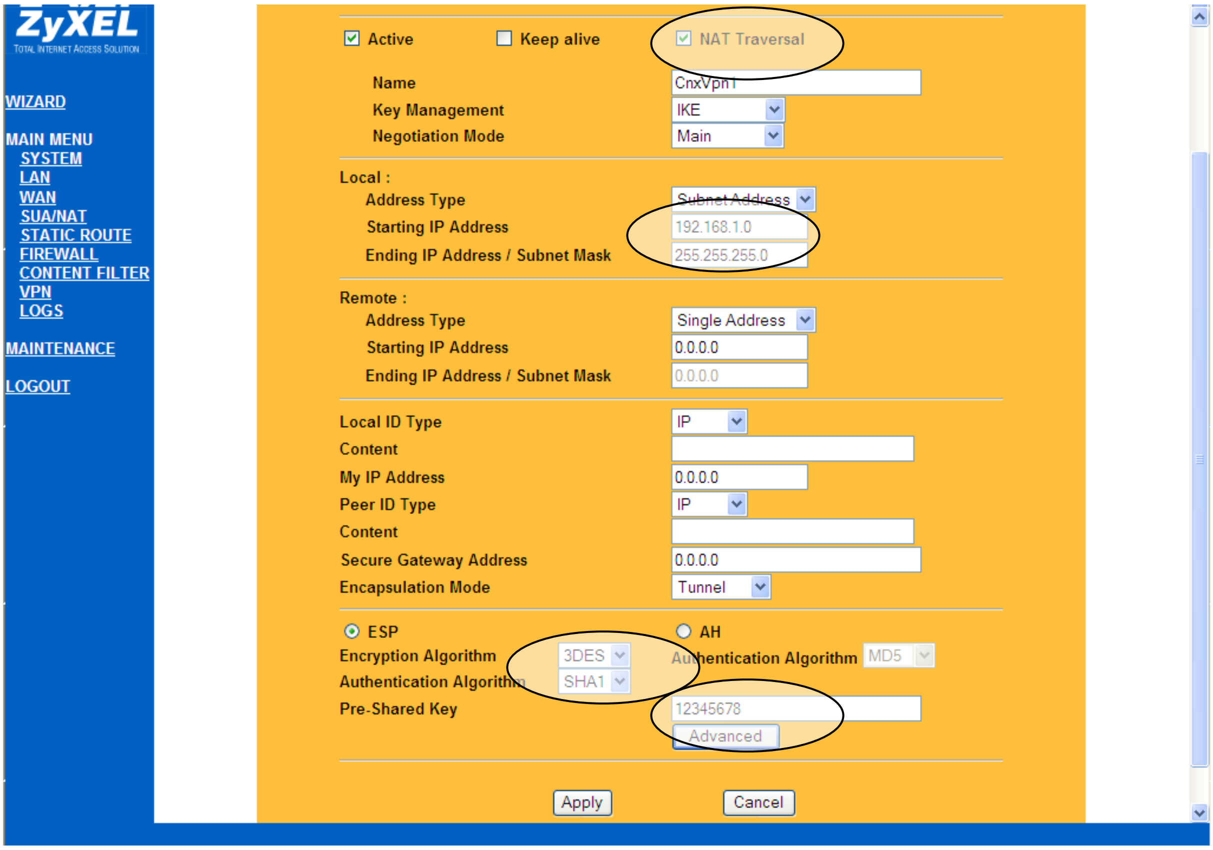
Then, go to 'VPN' under menu 'CONTENT FILTER' and select 'Add New Policy'.



VPN

	#	Name	Active	Local IP Address	Remote IP Address	Encap.	IPSec Algorithm	Secure Gateway Address
●	1	-	-	-	-	-	-	. . .
○	2	-	-	-	-	-	-	. . .
○	3	-	-	-	-	-	-	. . .
○	4	-	-	-	-	-	-	. . .
○	5	-	-	-	-	-	-	. . .
○	6	-	-	-	-	-	-	. . .
○	7	-	-	-	-	-	-	. . .
○	8	-	-	-	-	-	-	. . .
○	9	-	-	-	-	-	-	. . .
○	10	-	-	-	-	-	-	. . .

Click on 'Edit'.



☑ Active ☐ Keep alive ☑ NAT Traversal

Name: CnxVpn1
Key Management: IKE
Negotiation Mode: Main

Local :
Address Type: Subnet Address
Starting IP Address: 192.168.1.0
Ending IP Address / Subnet Mask: 255.255.255.0

Remote :
Address Type: Single Address
Starting IP Address: 0.0.0.0
Ending IP Address / Subnet Mask: 0.0.0.0

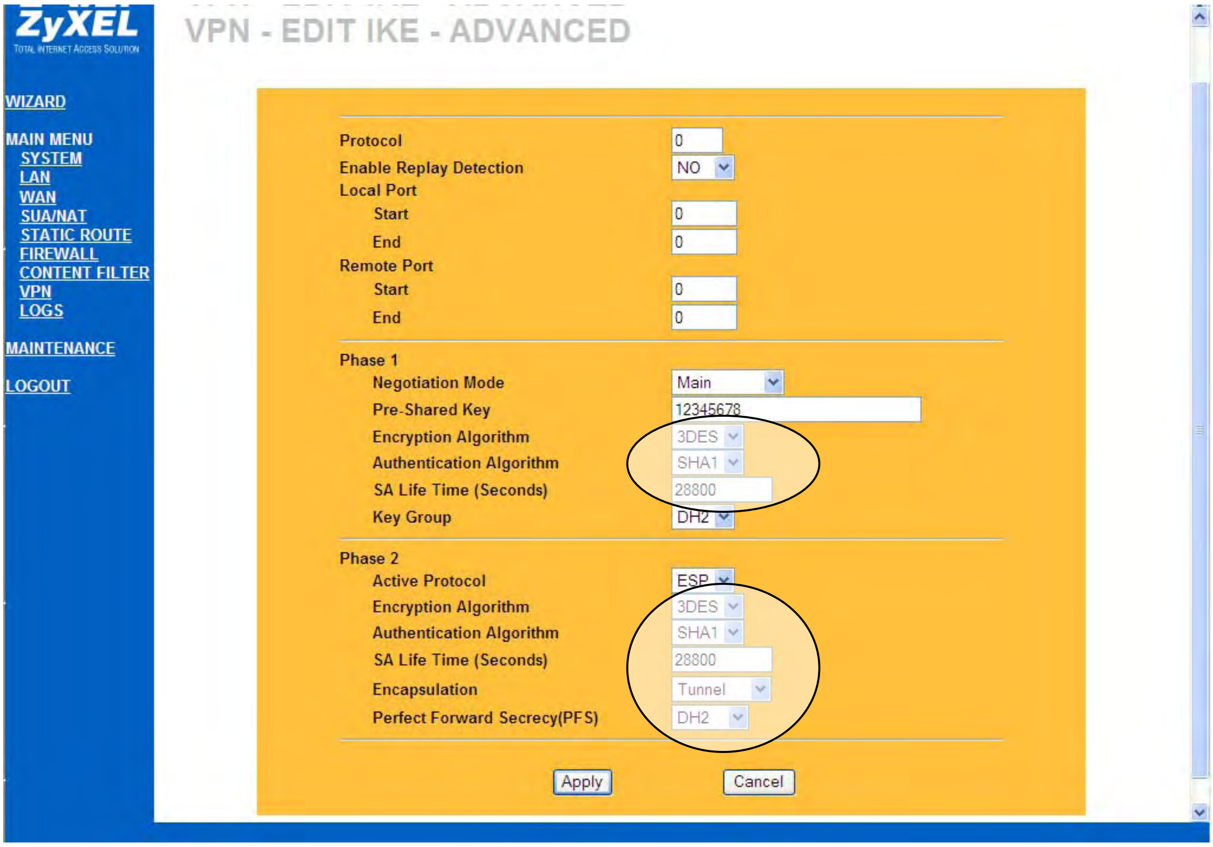
Local ID Type: IP
Content:
My IP Address: 0.0.0.0
Peer ID Type: IP
Content:
Secure Gateway Address: 0.0.0.0
Encapsulation Mode: Tunnel

● ESP ○ AH
Encryption Algorithm: 3DES
Authentication Algorithm: SHA1
Authentication Algorithm: MD5
Pre-Shared Key: 12345678

So in the part ‘Local’ you put the Local LAN Address. Select ‘NAT Traversal’.

Then, you configure the ESP algorithms with 3DES, SHA and you choose a Preshared Key: 12345678.

Once done, you click on ‘Advanced’ to configure other parameters required into TheGreenBow IPSec VPN Client.



VPN - EDIT IKE - ADVANCED

Protocol	0
Enable Replay Detection	NO
Local Port	
Start	0
End	0
Remote Port	
Start	0
End	0
Phase 1	
Negotiation Mode	Main
Pre-Shared Key	12345678
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
SA Life Time (Seconds)	28800
Key Group	DH2
Phase 2	
Active Protocol	ESP
Encryption Algorithm	3DES
Authentication Algorithm	SHA1
SA Life Time (Seconds)	28800
Encapsulation	Tunnel
Perfect Forward Secrecy(PFS)	DH2

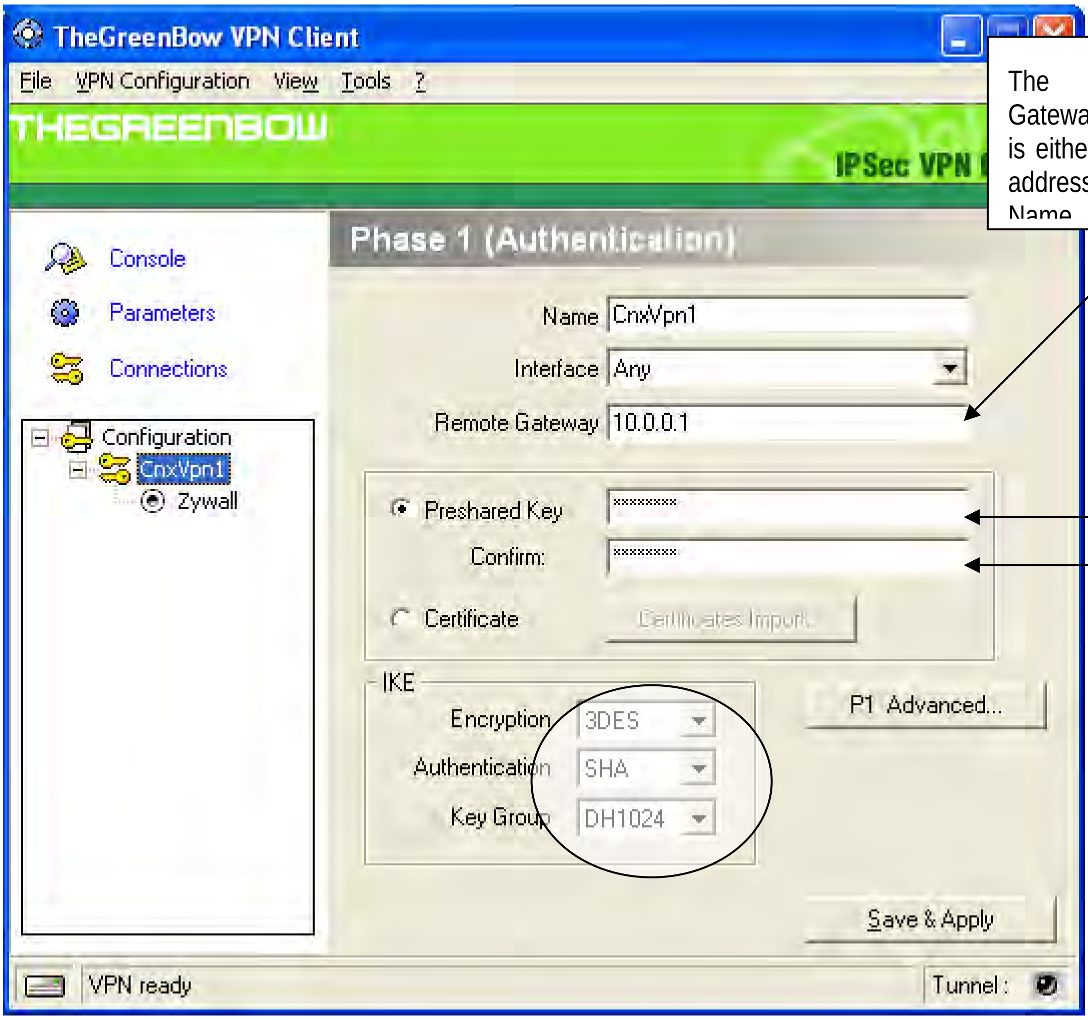
So here you find again the algorithms for each phase of TheGreenBow IPSec VPN Client. Click on ‘Apply’ when done.

3 TheGreenBow IPSec VPN Client configuration

This section describes the required configuration to connect to a Zyxel Zywall 10 VPN router.

To download the latest release of TheGreenBow IPSec VPN Client software, please go to http://www.thegreenbow.com/vpn_down.html.

3.1 VPN Client Phase 1 (IKE) Configuration



Name: CnxVpn1

Interface: Any

Remote Gateway: 10.0.0.1

● Preshared Key: ********

Confirm: ********

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA

Key Group: DH1024

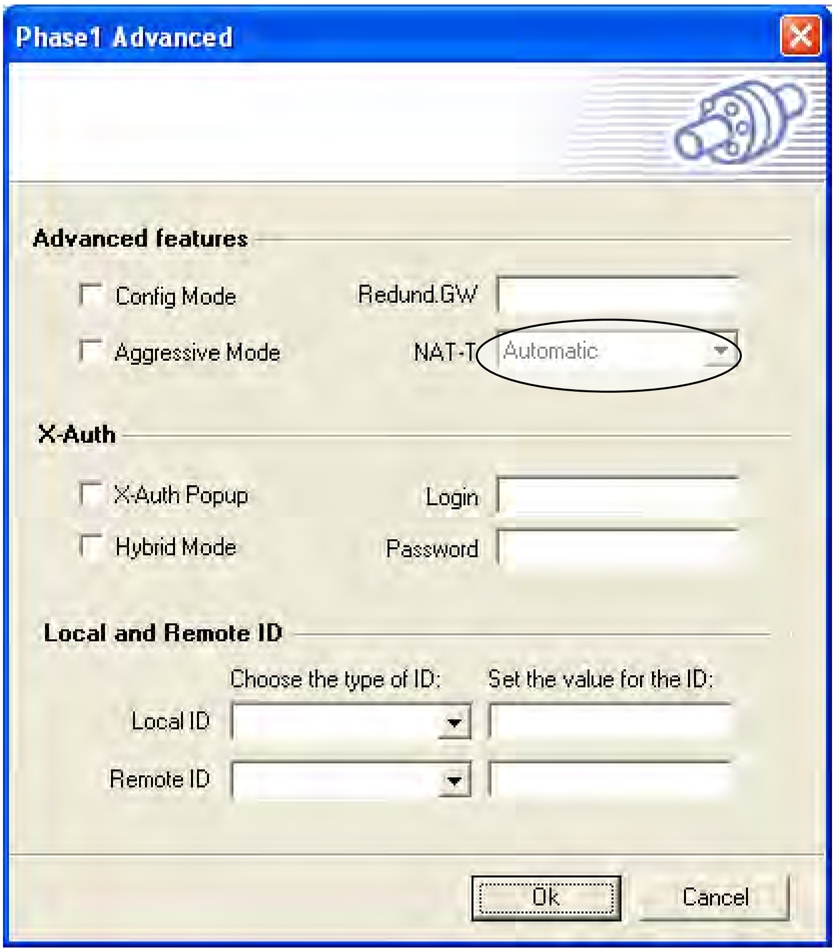
The remote VPN Gateway IP Address is either an explicit IP address, or a DNS Name

12345678

12345678

Phase 1 configuration

As configured in the router, we need to setup the same algorithms for IKE and the same PreShared key.



Phase1 Advanced

Advanced features

□ Config Mode

Redund.GW

□ Aggressive Mode

NAT-T Automatic

X-Auth

□ X-Auth Popup

Login

□ Hybrid Mode

Password

Local and Remote ID

Choose the type of ID:

Set the value for the ID:

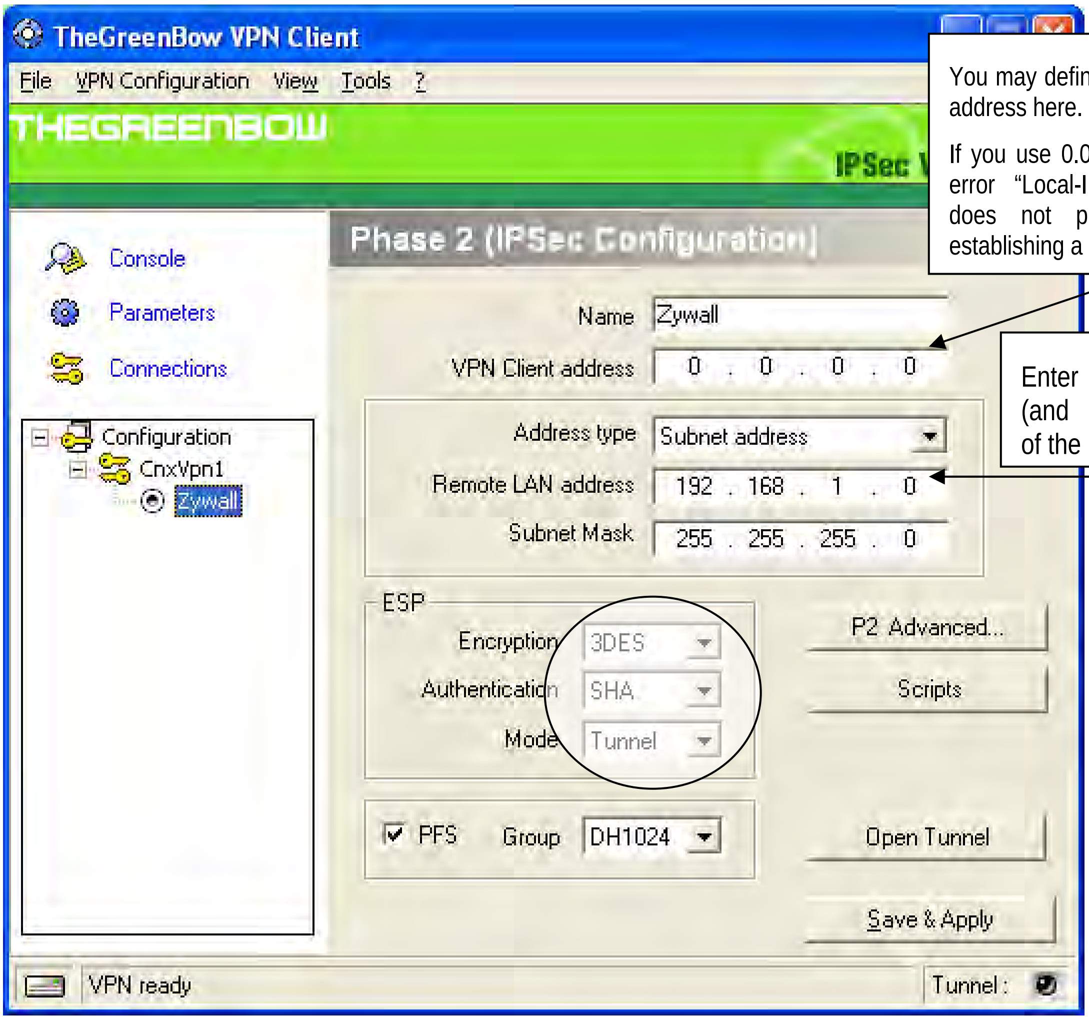
Local ID

Remote ID

Don’t forget to set ‘NAT-T’ to ‘Automatic’. Click on ‘Ok’.

Now, you’ve completed configuration of the Phase 1.

3.2 VPN Client Phase 2 (IPSec) Configuration



Name: Zywall

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: 3DES

Authentication: SHA

Mode: Tunnel

☑ PFS Group: DH1024

You may define a static virtual IP address here.

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

Enter the IP address (and subnet mask) of the remote LAN.

Phase 2 Configuration

The part ESP shall match the Phase2 group in the Zywall VPN router.

3.3 Open IPSec VPN tunnels

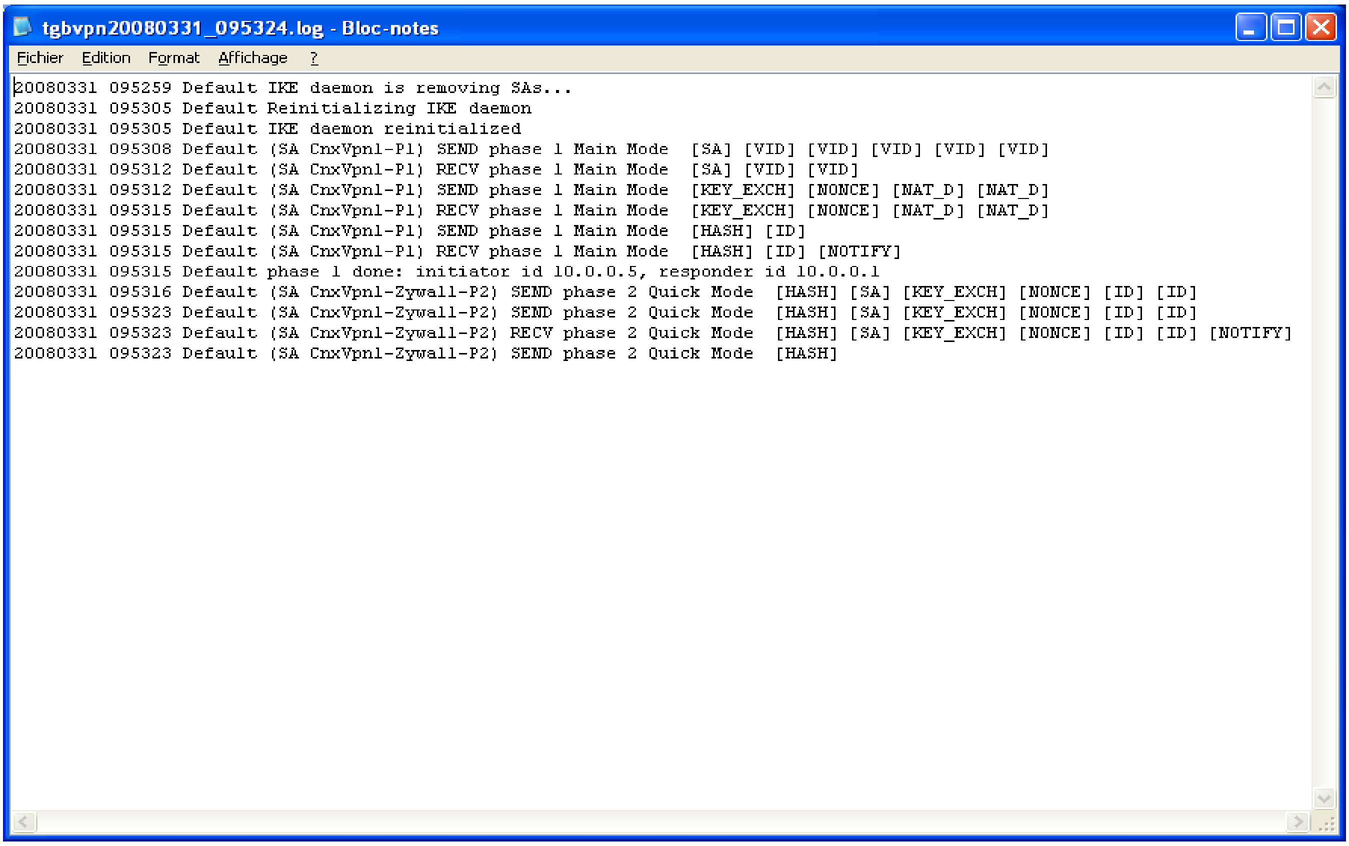
Once both Zyxel Zywall 10 router and TheGreenBow IPSec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPSec traffic.

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**" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Zyxel Zywall 10 VPN router.



tgbvpn20080331_095324.log - Bloc-notes
Fichier Edition Format Affichage ?

```
20080331 095259 Default IKE daemon is removing SAs...
20080331 095305 Default Reinitializing IKE daemon
20080331 095305 Default IKE daemon reinitialized
20080331 095308 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode  [SA] [VID] [VID] [VID] [VID] [VID]
20080331 095312 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode  [SA] [VID] [VID]
20080331 095312 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080331 095315 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode  [KEY_EXCH] [NONCE] [NAT_D] [NAT_D]
20080331 095315 Default (SA CnxVpn1-P1) SEND phase 1 Main Mode  [HASH] [ID]
20080331 095315 Default (SA CnxVpn1-P1) RECV phase 1 Main Mode  [HASH] [ID] [NOTIFY]
20080331 095315 Default phase 1 done: initiator id 10.0.0.5, responder id 10.0.0.1
20080331 095316 Default (SA CnxVpn1-Zywall-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080331 095323 Default (SA CnxVpn1-Zywall-P2) SEND phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID]
20080331 095323 Default (SA CnxVpn1-Zywall-P2) RECV phase 2 Quick Mode  [HASH] [SA] [KEY_EXCH] [NONCE] [ID] [ID] [NOTIFY]
20080331 095323 Default (SA CnxVpn1-Zywall-P2) SEND phase 2 Quick Mode  [HASH]
```

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: Wireshark

Wireshark 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 http://www.wireshark.org. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (http://www.wireshark.org/docs/).

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 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.

5.2 « 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.

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 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.

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  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.

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 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
```

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
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).

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 support ESP

- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark 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 Wireshark (http://www.wireshark.org) on one of your target computer. You can check that your pings arrive inside the LAN.

6 Contacts

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

Technical support by email at support@thegreenbow.com

Sales contacts by email at sales@thegreenbow.com