TheGreenBow IPSec VPN Client

Configuration Guide

CNET CWR-854 firmware v1.2.3.3

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

Table of contents

1 Introduction

1.1 Goal of this document

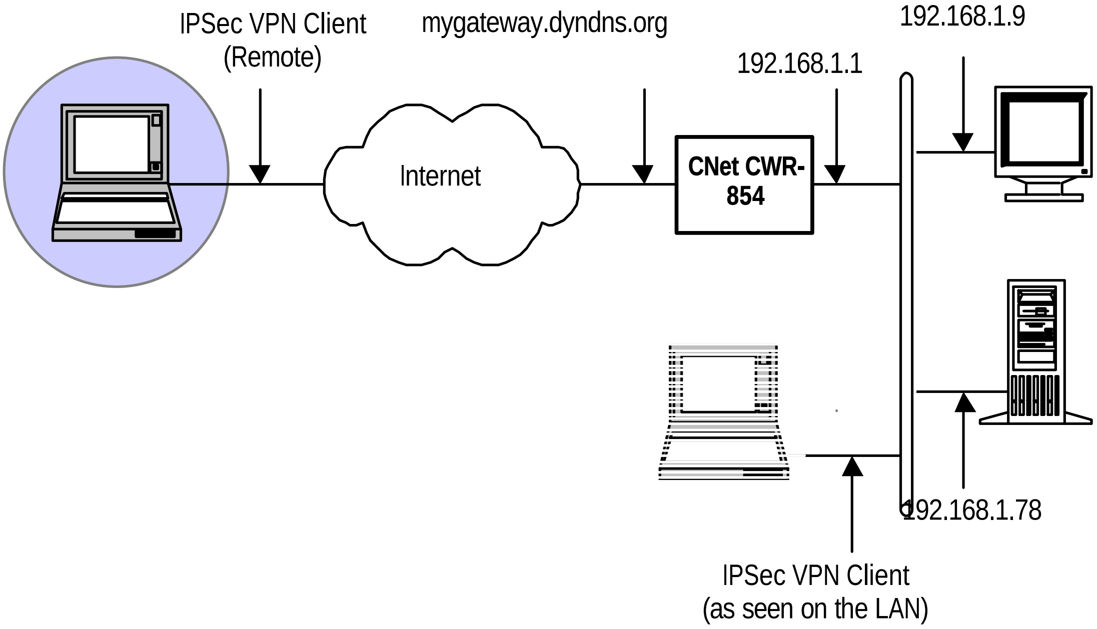
This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a CNet CWR-854 VPN gateway running firmware v1.2.3.3

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the CWR-854 gateway. 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.

A Road Warrior connection also needs to be configured. The following example makes use of these values:

? External IP of the CWR-854:	mygateway.dyndns.org (or public IP address)
? IP Subnet behind the CNet CWR-854:	192.168.1.0/255.255.255.0

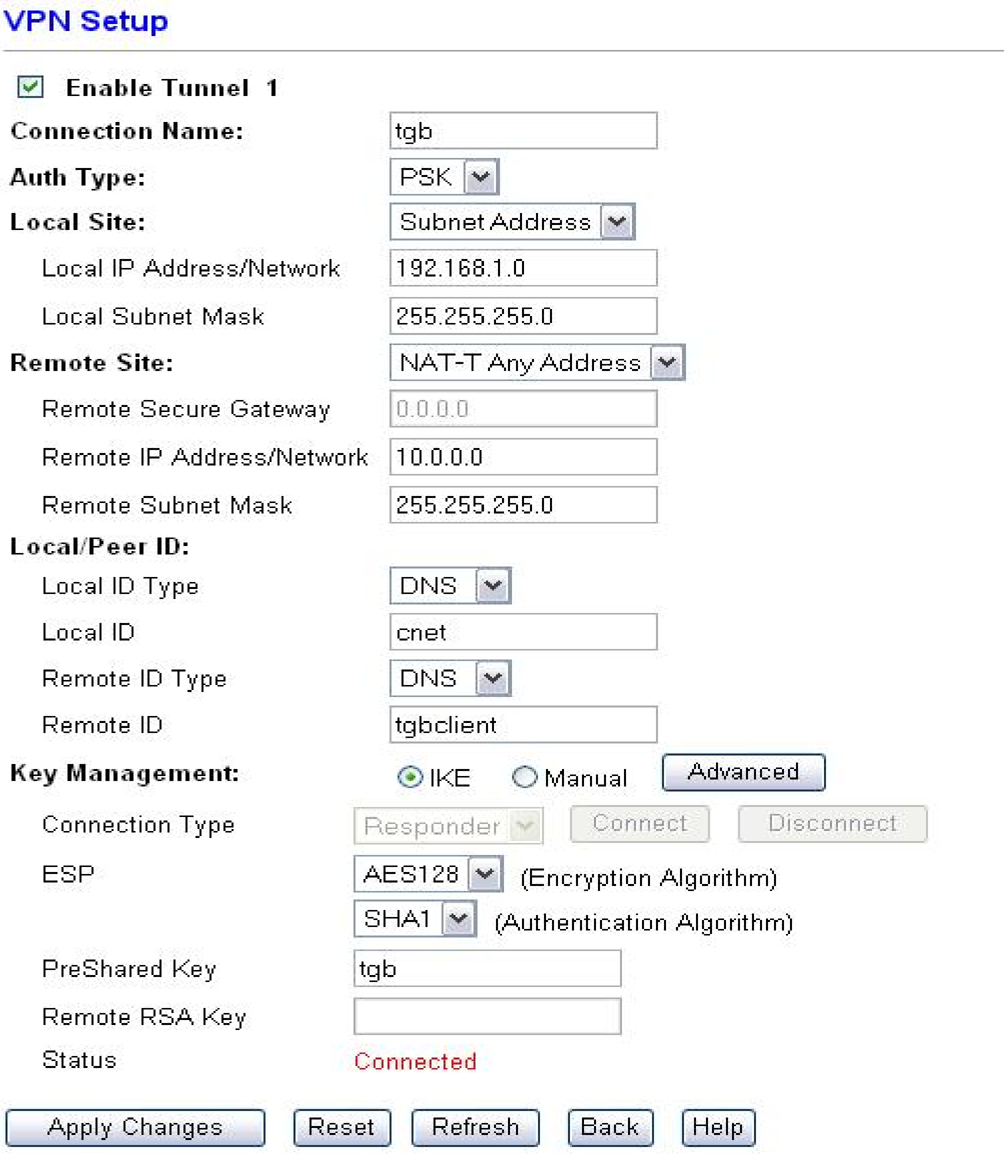


2 Configuring IPSec Road Warrior connection with CNet CW-854

This section describes how to build an IPSec VPN configuration with your CNet CWR-854 VPN Gateway.

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

Below is a screenshot of a configuration made with the values used above.

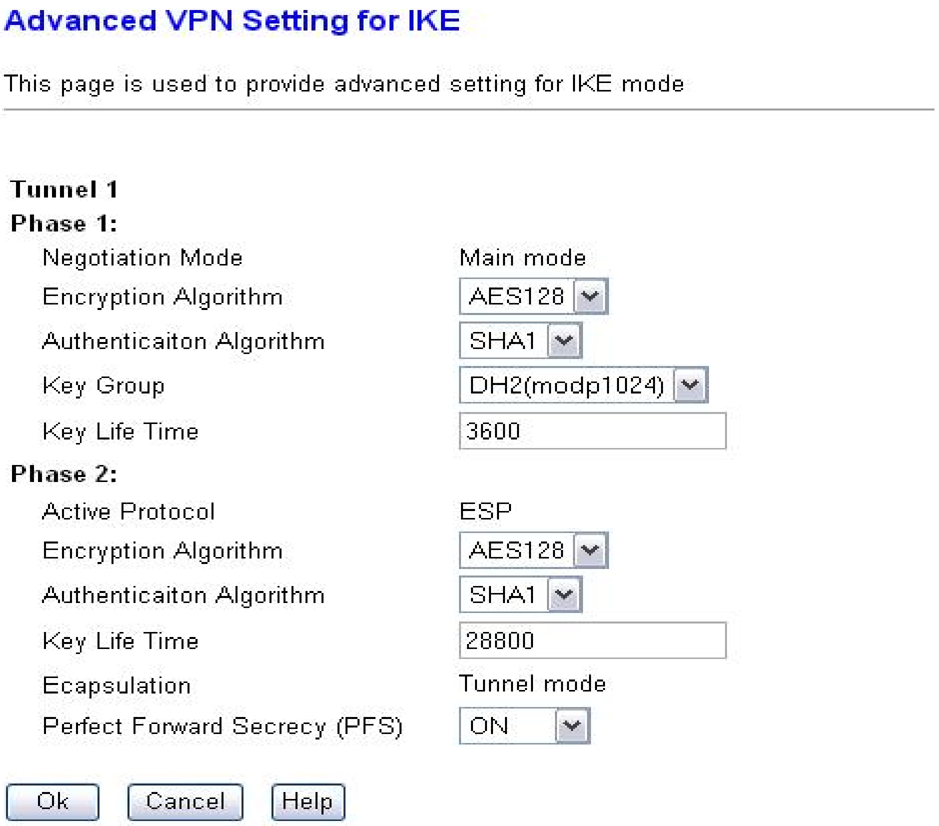


VPN Setup

☑ Enable Tunnel 1

Connection Name:	tgb
Auth Type:	PSK
Local Site:	Subnet Address
Local IP Address/Network	192.168.1.0
Local Subnet Mask	255.255.255.0
Remote Site:	NAT-T Any Address
Remote Secure Gateway	0.0.0.0
Remote IP Address/Network	10.0.0.0
Remote Subnet Mask	255.255.255.0
Local/Peer ID:	
Local ID Type	DNS
Local ID	cnet
Remote ID Type	DNS
Remote ID	tgbclient
Key Management:	● IKE ○ Manual Advanced
Connection Type	Responder Connect Disconnect
ESP	AES128 (Encryption Algorithm) SHA1 (Authentication Algorithm)
PreShared Key	tgb
Remote RSA Key	
Status	Connected

The same preshared key must be entered in TheGreenBow vpn client Phase1



Advanced VPN Setting for IKE

This page is used to provide advanced setting for IKE mode

Tunnel 1

Phase 1:

Negotiation Mode	Main mode
Encryption Algorithm	AES128
Authenticaiton Algorithm	SHA1
Key Group	DH2(modp1024)
Key Life Time	3600

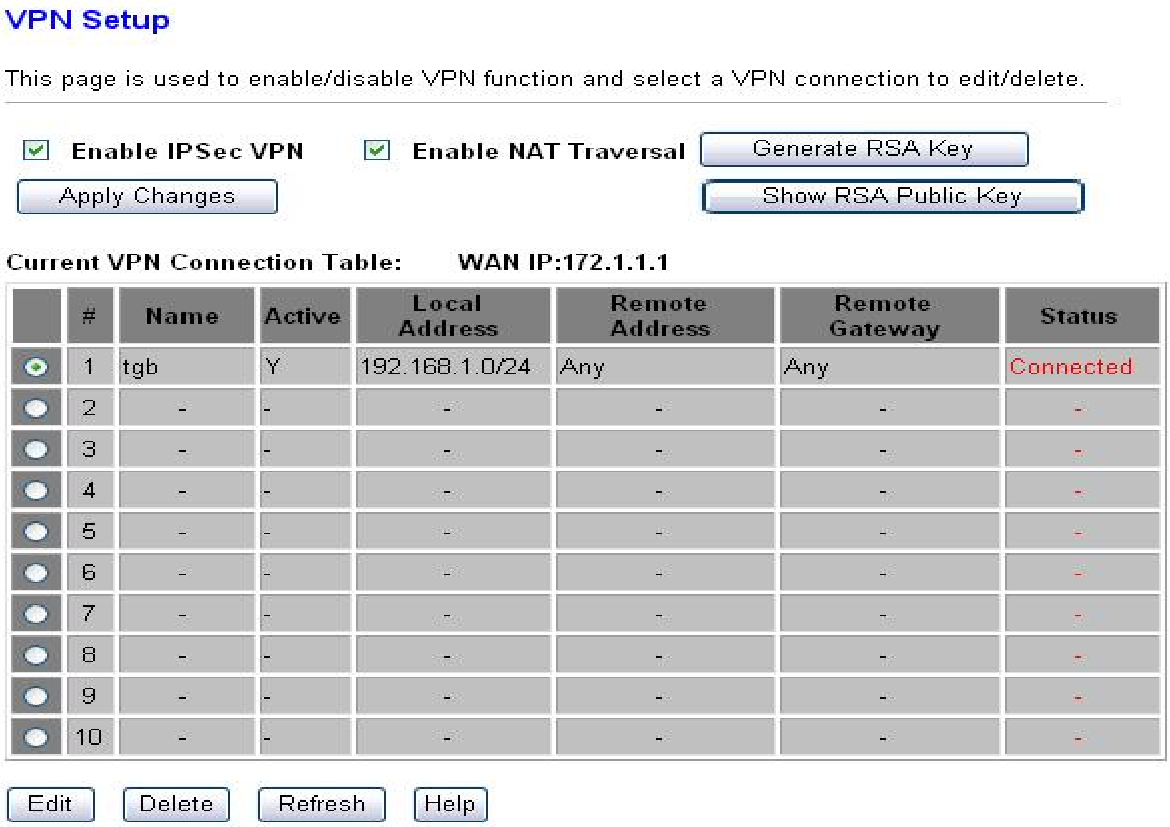
Phase 2:

Active Protocol	ESP
Encryption Algorithm	AES128
Authenticaiton Algorithm	SHA1
Key Life Time	28800
Ecapsulation	Tunnel mode
Perfect Forward Secrecy (PFS)	ON

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.

Here is an overview of the vpn with CNet CWR-854:



VPN Setup

This page is used to enable/disable VPN function and select a VPN connection to edit/delete.

☑ Enable IPSec VPN ☑ Enable NAT Traversal

Current VPN Connection Table: WAN IP:172.1.1.1

	#	Name	Active	Local Address	Remote Address	Remote Gateway	Status
●	1	tgb	Y	192.168.1.0/24	Any	Any	Connected
○	2	-	-	-	-	-	-
○	3	-	-	-	-	-	-
○	4	-	-	-	-	-	-
○	5	-	-	-	-	-	-
○	6	-	-	-	-	-	-
○	7	-	-	-	-	-	-
○	8	-	-	-	-	-	-
○	9	-	-	-	-	-	-
○	10	-	-	-	-	-	-

Wan IP address matches Phase1 remote gateway address.

3 TheGreenBow IPSec VPN Client configuration

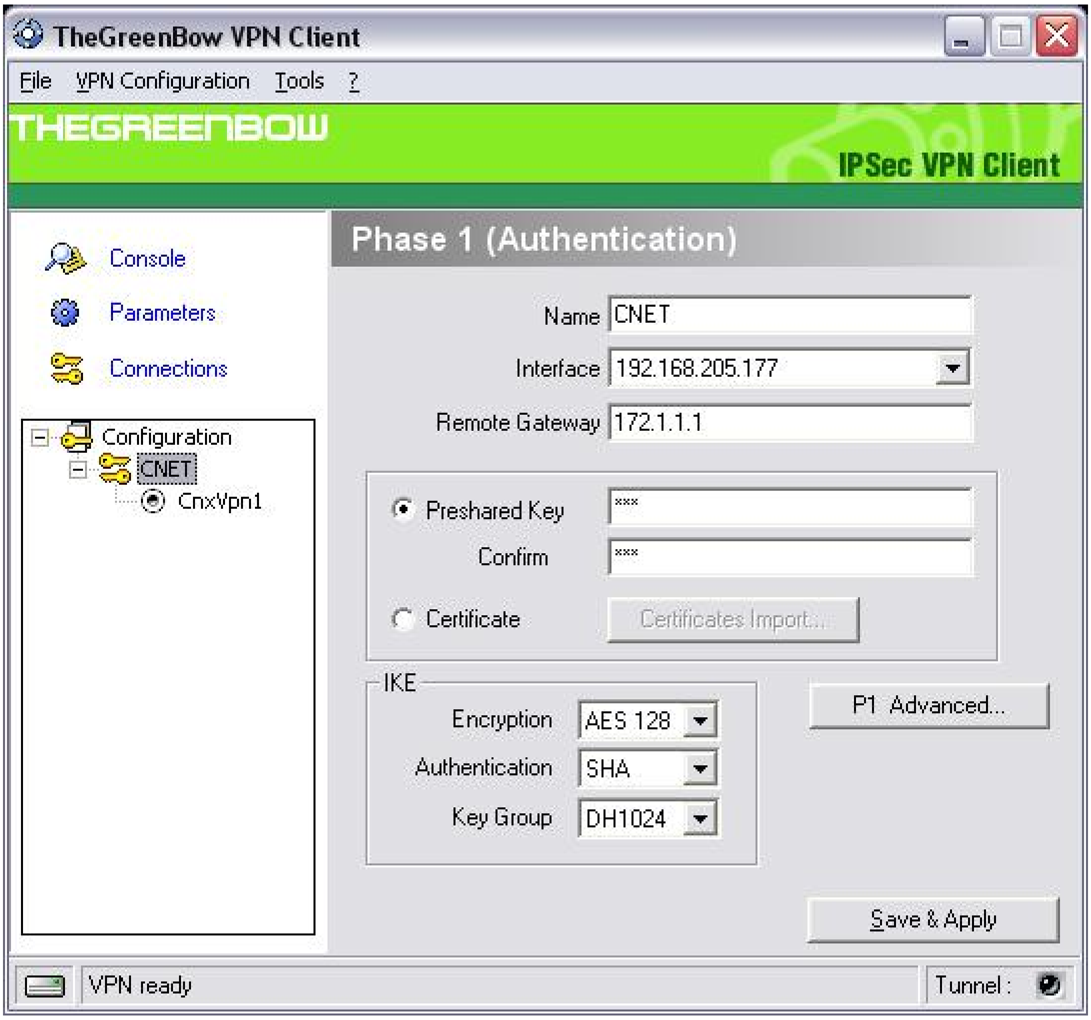
3.1 VPN Client Phase 1 Configuration

Now lets add a Phase 1 to the CNET connection. Right click on Configuration in **TheGreenbow** VPN client and select "**Add Phase 1**".

Then select the "new phase 1" screen. The values that need to be changed and entered are displayed here:

The preshared key used in this example is intentionally short. Don t use this key length in a production environement, it must be complex enough for maximum security.

Phase 1 Configuration



Name: CNET

Interface: 192.168.205.177

Remote Gateway: 172.1.1.1

● Preshared Key: ***

Confirm: ***

○ Certificate

IKE

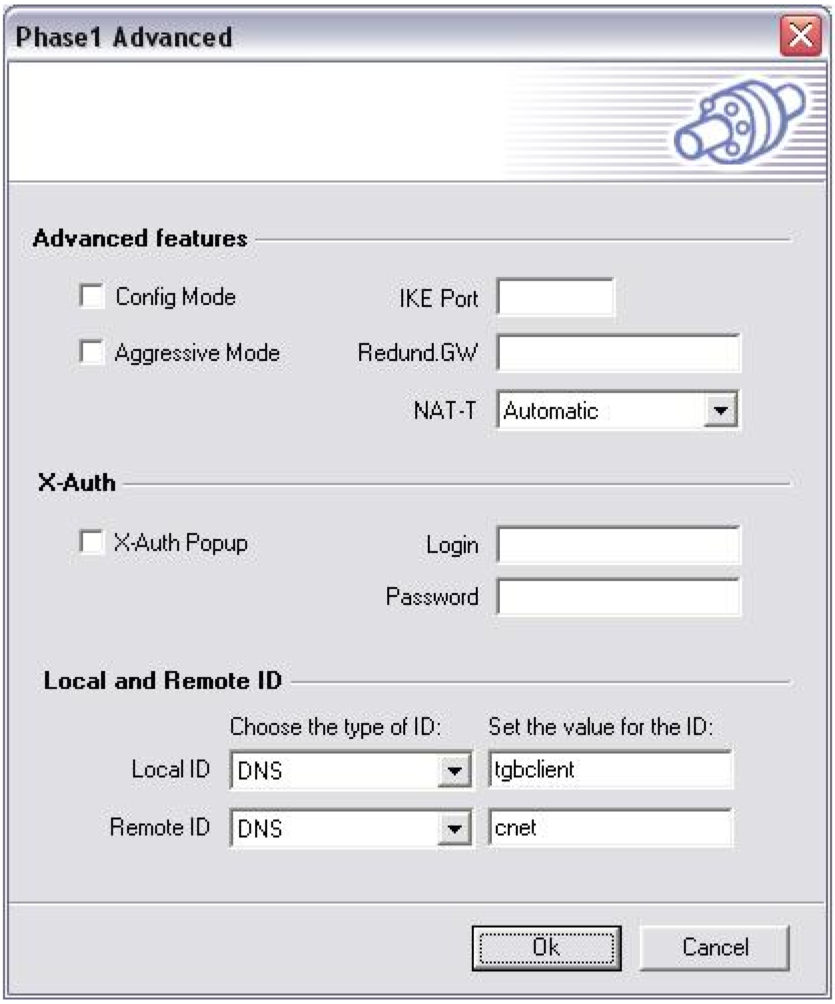
Encryption: AES 128

Authentication: SHA

Key Group: DH1024

VPN ready

IP address 172.1.1.1 was used because of the test platform (Cnet + vpn client) being internal to our network, you MUST change it to match your dyndns or fixed public ip address.



Phase1 Advanced

Advanced features

□ Config Mode

□ Aggressive Mode

IKE Port

Redund.GW

NAT-T: Automatic

X-Auth

□ X-Auth Popup

Login

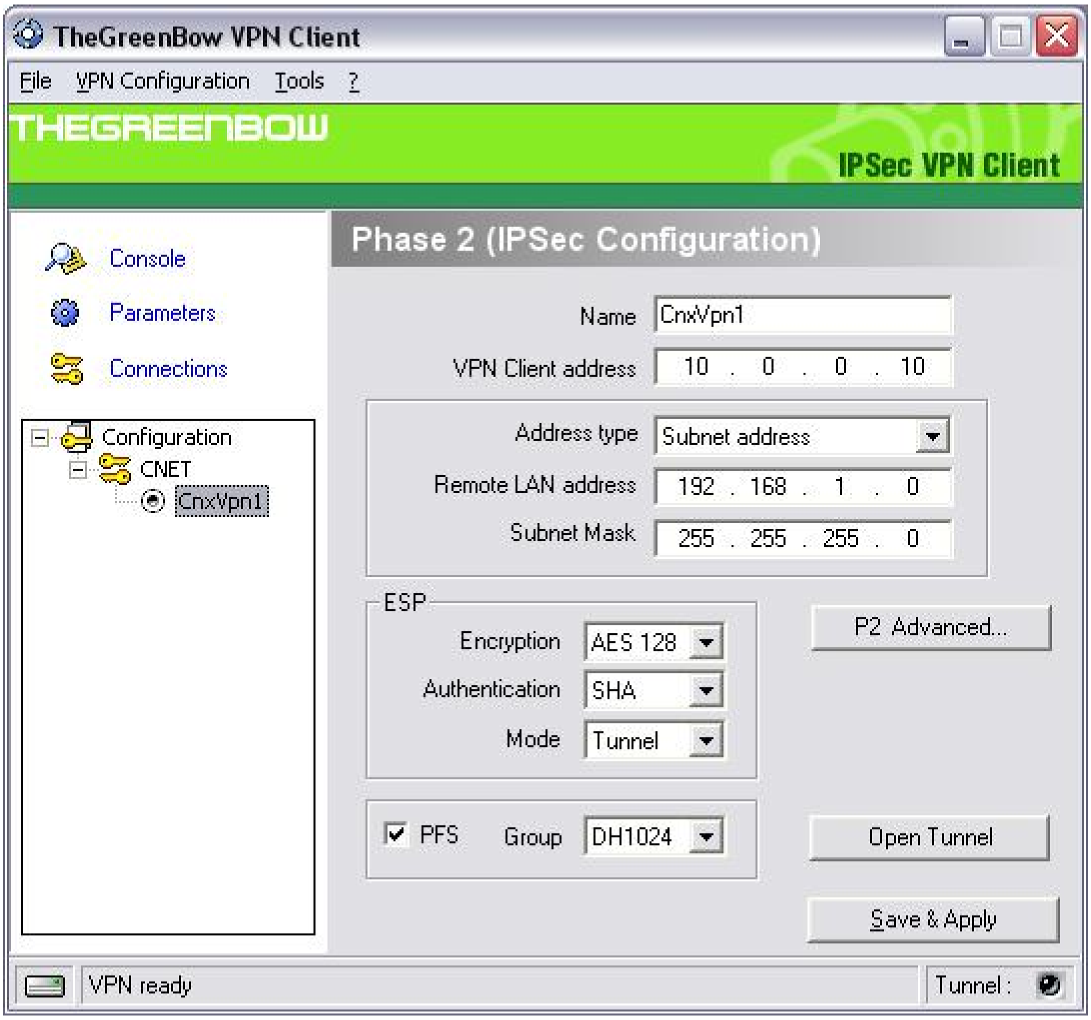
Password

Local and Remote ID

	Choose the type of ID:	Set the value for the ID:
Local ID	DNS	tgbclient
Remote ID	DNS	cnet

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 anything (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: CnxVpn1

VPN Client address: 10 . 0 . 0 . 10

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: DH1024

VPN ready

The VPN client address must not belong to the remote subnet range.

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.

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