TheGreenBow IPSec VPN Client

Configuration Guide

Planet CS-1000

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

Table of contents

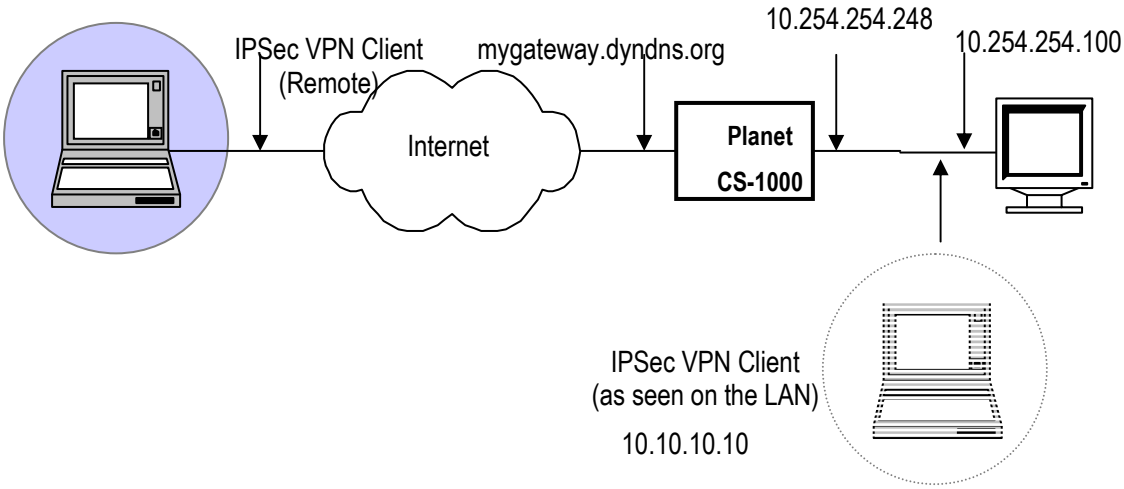
1. Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a Planet CS-1000 Multi-Homing Security Gateway

1.2 VPN Network topology

- Planet CS-1000 External IP : mygateway.dyndns.org (or static public IP address)
- Planet CS-1000 Internal IP: 10.254.254.248
- Subnet behind Planet CS-1000: 10.254.254.0 / 255.255.255.0
- VPN client virtual IP (phase 2) : 10.10.10.10



2 Setup Planet CS-1000

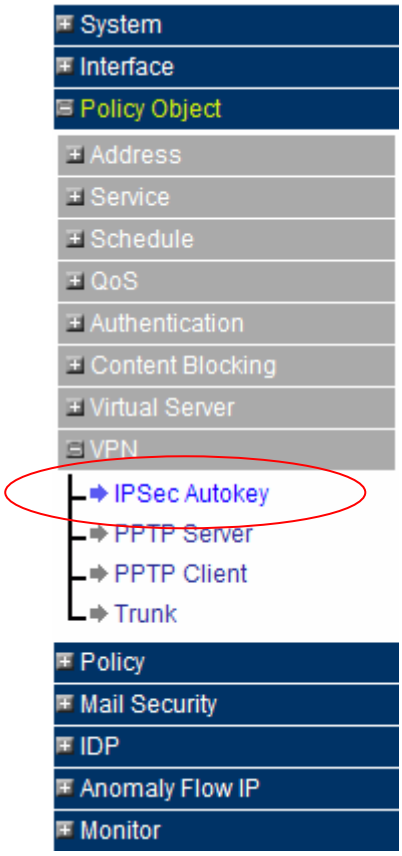
This section describes how to build an IPSec VPN configuration with Planet CS-1000 VPN Gateway.

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

We need to setup an IPSec AutoKey, and a Trunk Policy

2.1 IPSec AutoKey

Create a new IPSec Autokey policy on the CS-1000 .



Necessary Item	
Name	thegreenbow
WAN interface	(•) WAN 1 ( ) WAN 2
To Destination	
( ) Remote Gateway -- Fixed IP or Domain Name	( ) (Max. 99 characters)
(•) Remote Gateway or Client -- Dynamic IP	
Authentication Method	Preshare
Preshared Key	tgb2007 (Max. 103 characters)
Encapsulation	
ISAKMP Algorithm	
ENC Algorithm	AES-128
AUTH Algorithm	SHA1
Group	GROUP 2
IPSec Algorithm	
(•) Data Encryption + Authentication	
ENC Algorithm	AES-128
AUTH Algorithm	SHA1
( ) Authentication Only	

Optional Item	
Perfect Forward Secrecy	GROUP 2
ISAKMP Lifetime	28800 Seconds (Range: 1200 - 86400)
IPSec Lifetime	28800 Seconds (Range: 1200 - 86400)
Mode	(•) Main mode ( ) Aggressive mode
My ID	(Max. 39 characters)
Peer ID	(Max. 39 characters)
GRE/IPSec	
GRE Local IP	
GRE Remote IP	
[ ] Manual Connect	
Dead Peer Detection delay 5 Second Timeout 5 Second (delay Range: 0 - 10, 0: means disable; Timeout Range: 1 - 100)	

We used “Main mode” instead of “Aggressive mode” because of the lack of security with “Aggressive” compared to “Main”. In aggressive mode, keys are exchanged in clear.

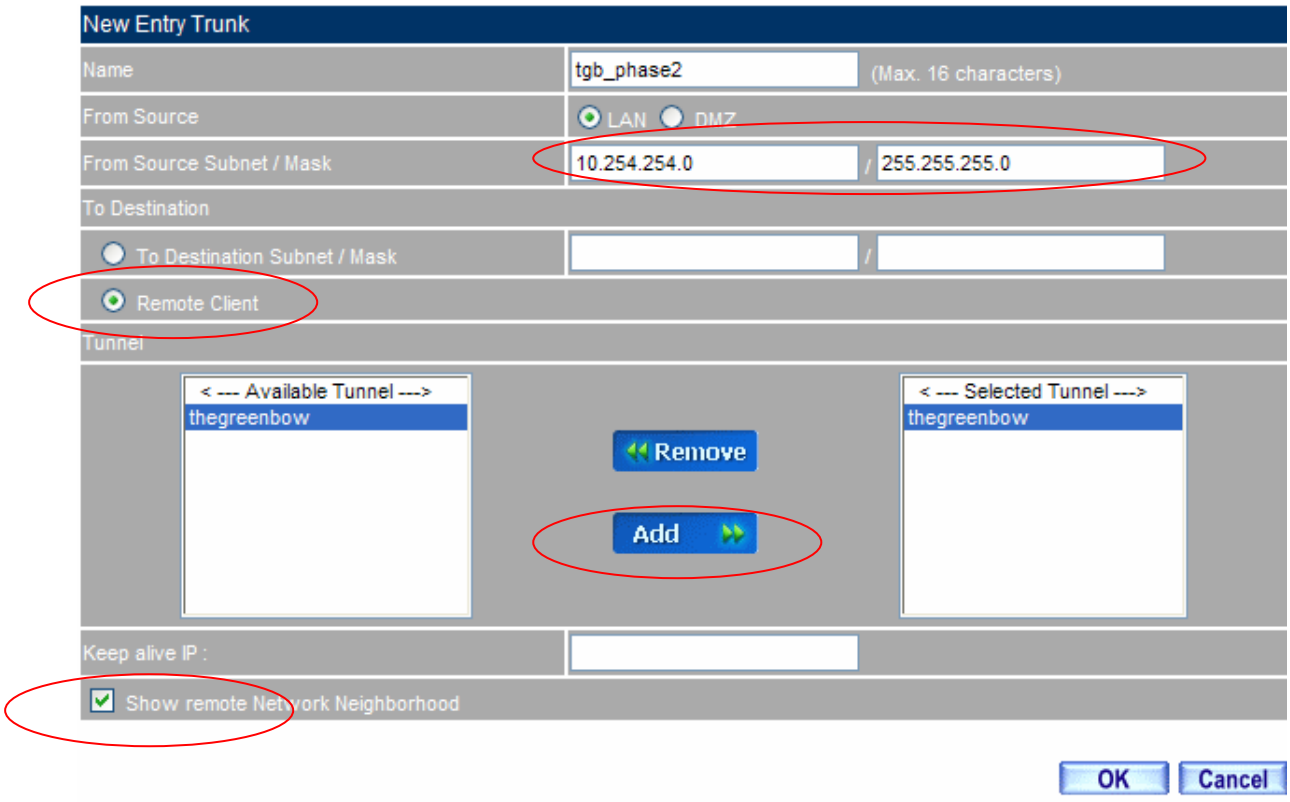
AES algorithm is more efficient than DES or 3DES (faster to cipher data and more secured), but anything else can be used.

If lifetimes are modified, it is recommended to tune ipsec and ike lifetimes accordingly on the vpn client (default values). This is found in Vpn configuration/ Parameters.

IDs fields are left blank in our example, security can be increased by entering local and remote IDs with IP address or FQDN (DNS) string type.

2.2 Trunk policy

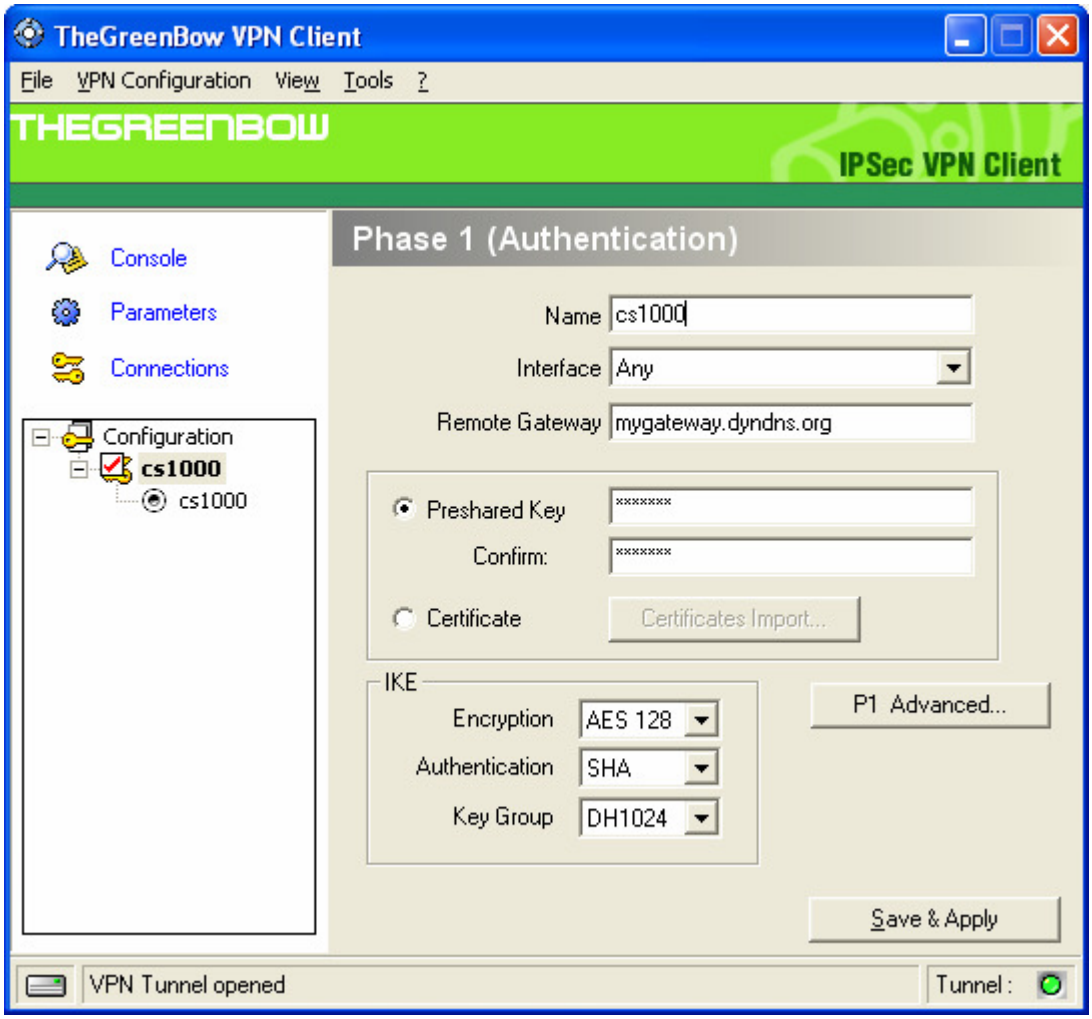
Create a New Entry Trunk , which in fact, is TheGreenBow vpn client's phase 2.



This is a traffic policy that needs to be linked to a tunnel definition. In our case there is only thegreenbow tunnel available. Phase 2 distant subnet on the vpn client must match the "Source Subnet/Mask" field on the newly created entry trunk.

3 TheGreenBow IPSec VPN Client configuration

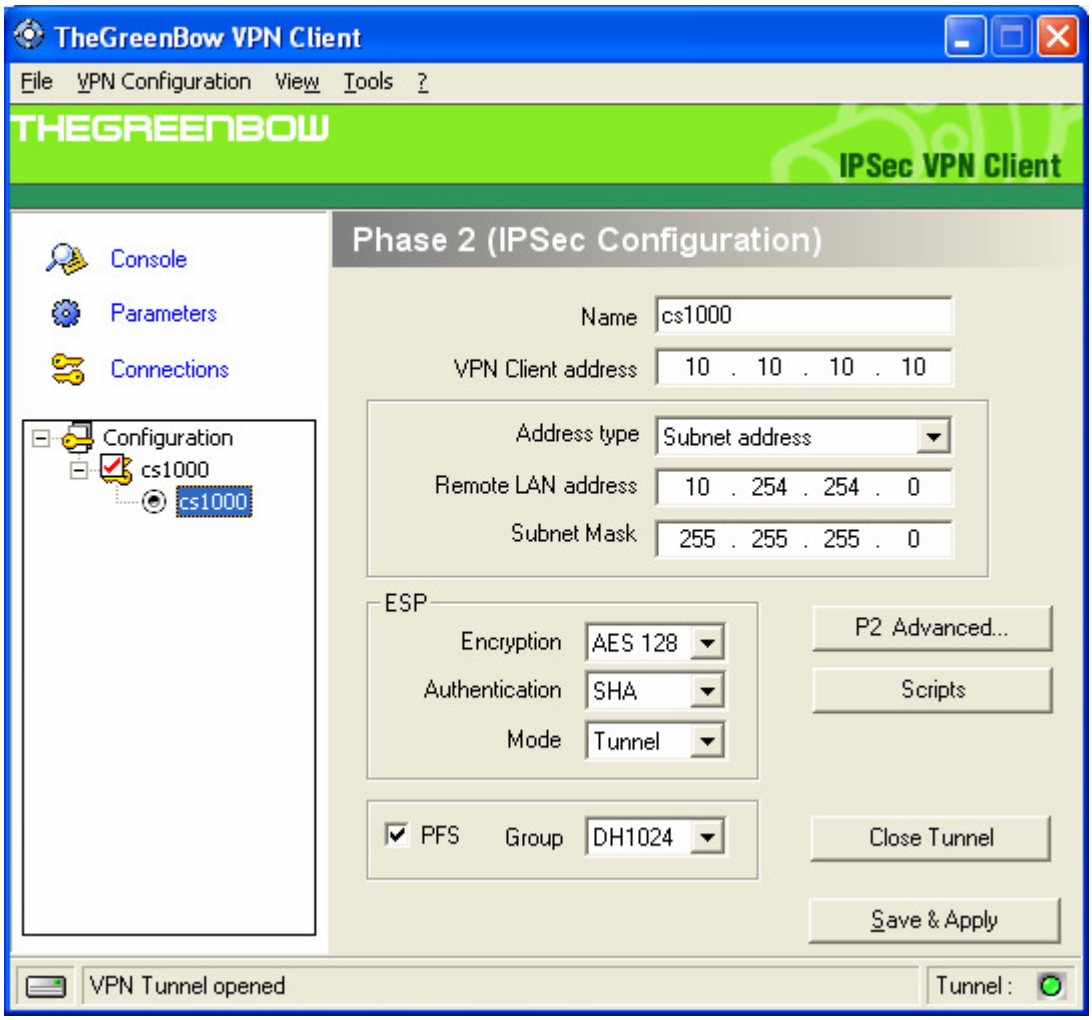
3.1 VPN Client Phase 1 Configuration



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

Click on “P1 Advanced…” to setup IDs if local and remote IDs were previously defined on the CS-1000.

3.2 VPN Client Phase 2 Configuration

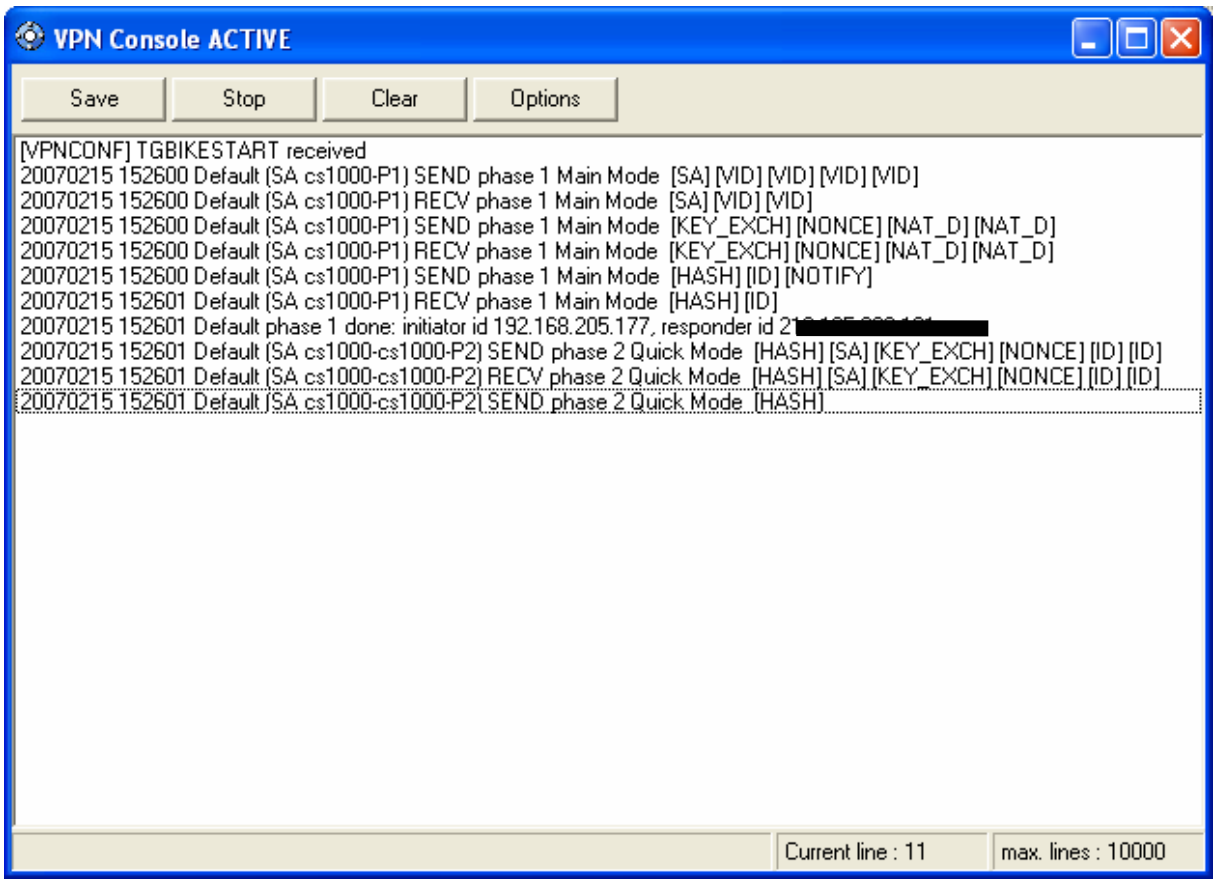


The VPN client address must not belong to the remote subnet range (virtual IP address 10.10.10.10).

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's screenshot below, shows a successful main mode vpn connection with the Planet CS-1000



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