TheGreenBow IPSec VPN Client

Configuration Guide

IPCop 1.4.16

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 free Linux distribution firewall downloadable from http://www.ipcop.org

This document is not a tutorial about IPCop installation as there are many "Howto" available on the internet.

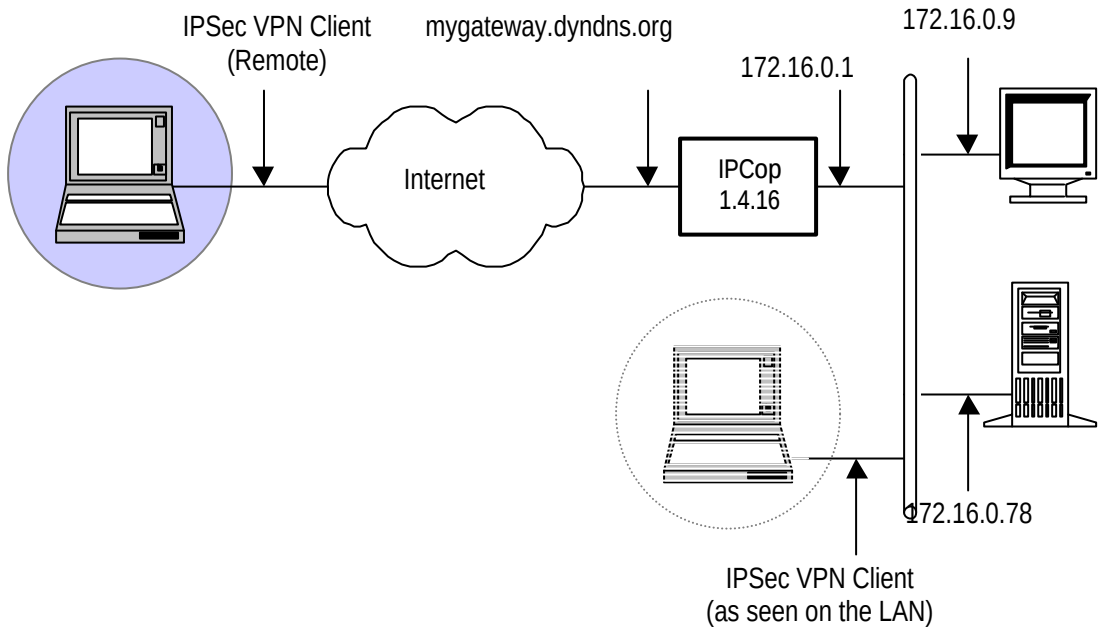
1.2 VPN Network topology

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

The network configuration chosen for IPCop is GREEN+ RED interfaces (LAN+WAN).

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

- External IP of the IPCop (red interface): mygateway.dyndns.org (or public IP address)
- IP Subnet behind the green interface (LAN): 172.16.0.0/255.255.255.0



1.3 IPCop VPN Gateway product info

It is critical that users find all necessary information about IPCop VPN Gateway. All product info, User Guide and knowledge base for the IPCop VPN Gateway can be found on the IPCop website: http://ipcop.org

IPCop Product page: http://ipcop.org/index.php?module=pnWikka&tag=IPCop14xFeatures

IPCop User Guide: http://ipcop.org/index.php?module=pnWikka&tag=IPCopDocumentation

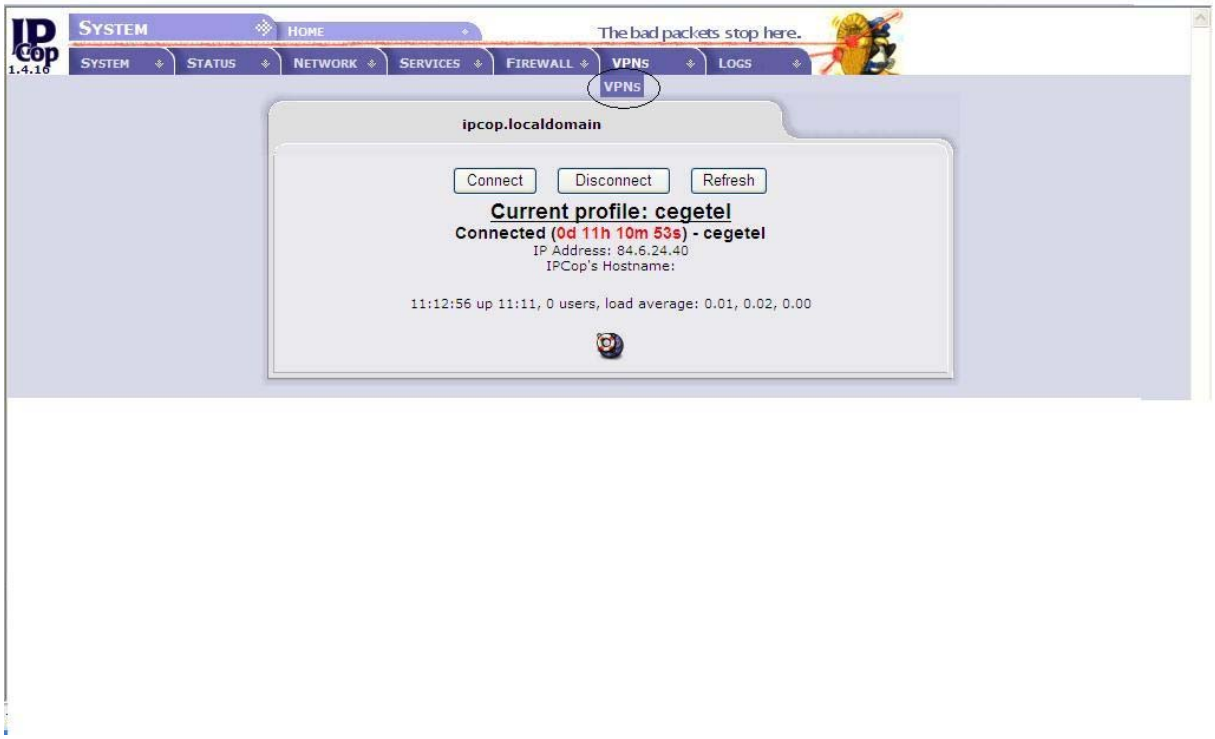
IPCop FAQ/Knowledge Base: http://ipcop.org/index.php?name=FAQ

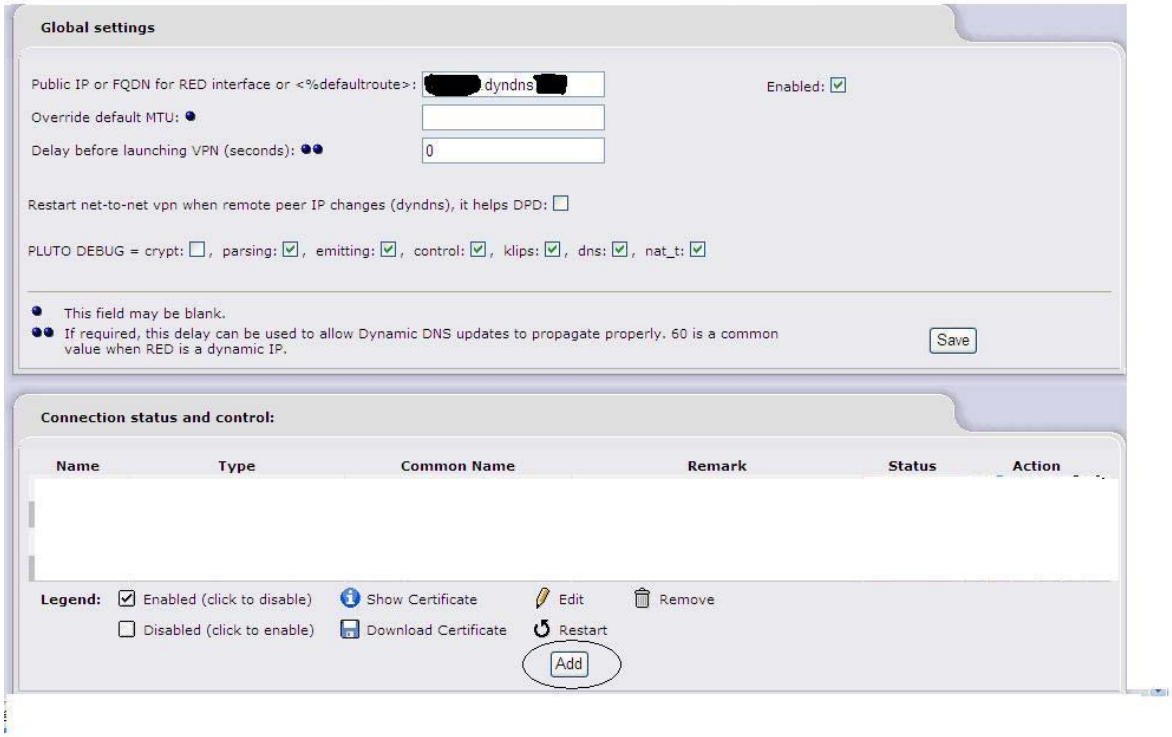
2 Setting up IPCop 1.4.16

2.1 Preparing IPCop's built

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

Once connected to your IPCop VPN gateway, go to VPNs tab.

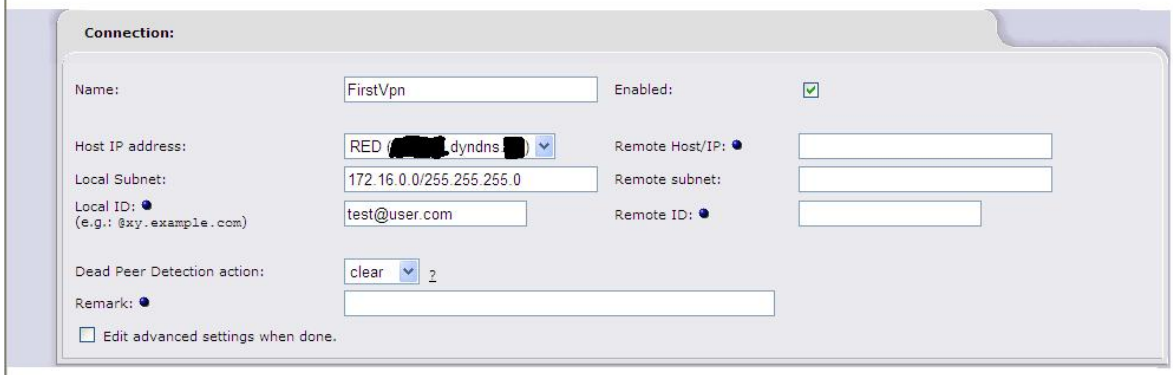


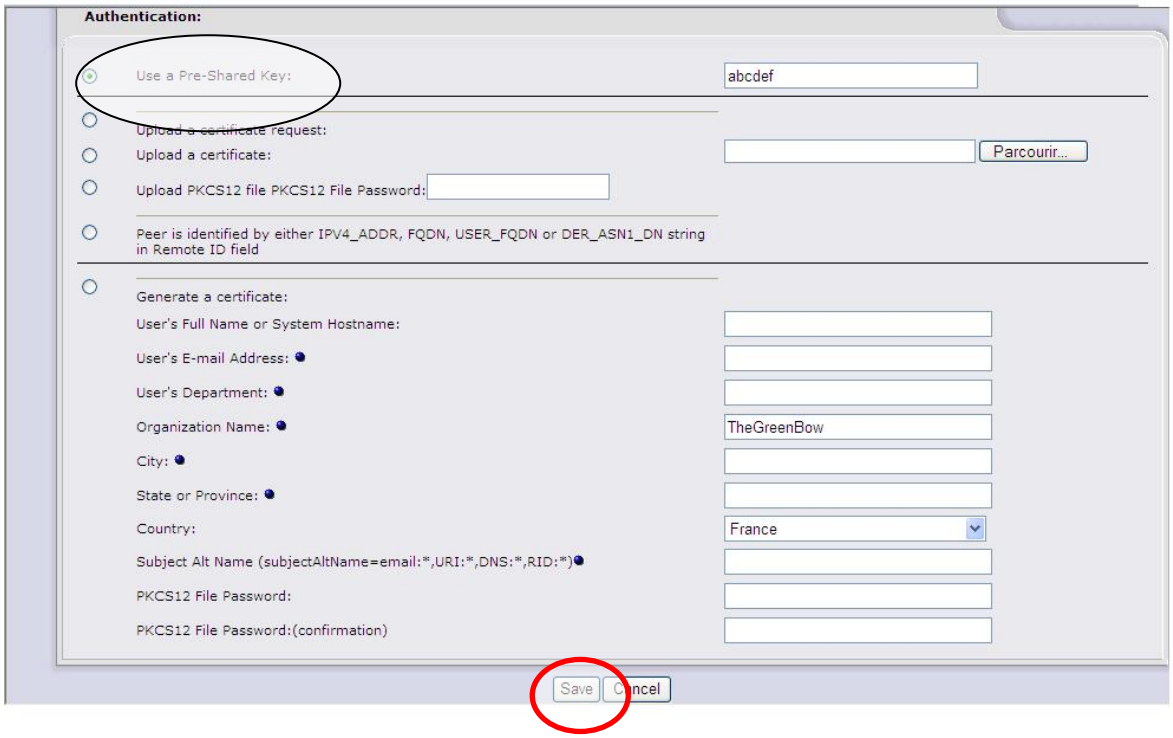


Press “Add” to configure a Roadwarrior connection

2.2 Setting up a Roadwarrior VPN Connection

Choose “Host-to-Net” VPN and press “Add”.

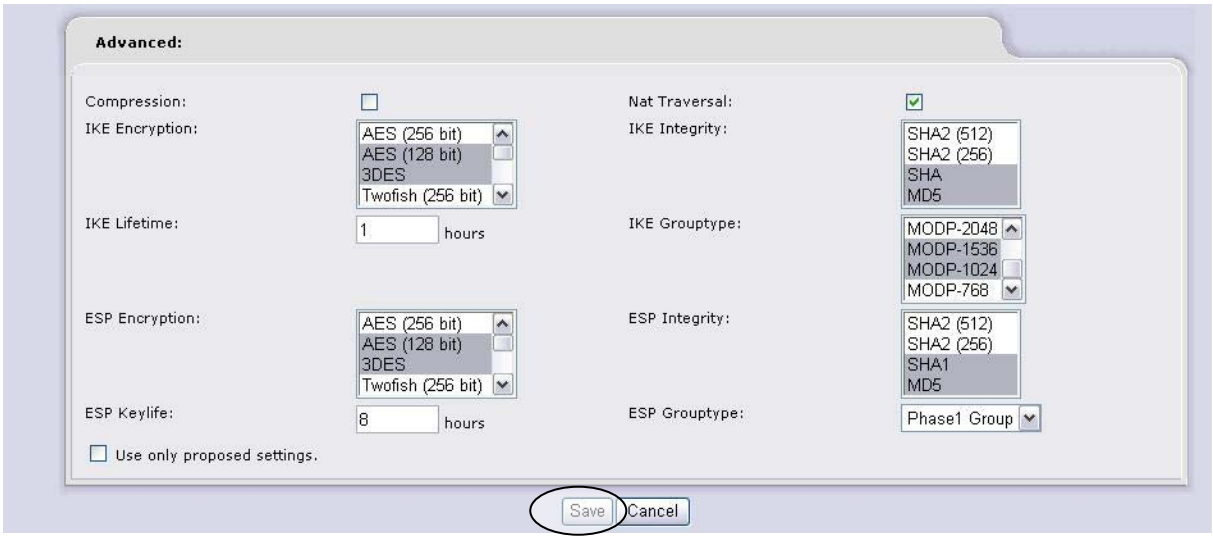

Connection:
Name:
FirstVpn
Enabled:
Host IP address:
RED
Remote Host/IP:
Local Subnet:
172.16.0.0/255.255.255.0
Remote subnet:
Local ID:
(e.g.: @xy.example.com)
test@user.com
Remote ID:
Dead Peer Detection action:
clear
Remark:
Edit advanced settings when done.


Authentication:
Use a Pre-Shared Key:
abcdef
Upload a certificate request:
Upload a certificate:
Parcourir...
Upload PKCS12 file PKCS12 File Password:
Peer is identified by either IPV4_ADDR, FQDN, USER_FQDN or DER_ASN1_DN string in Remote ID field
Generate a certificate:
User's Full Name or System Hostname:
User's E-mail Address:
User's Department:
Organization Name:
TheGreenBow
City:
State or Province:
Country:
France
Subject Alt Name (subjectAltName=email:*,URI:*,DNS:*,RID:*)
PKCS12 File Password:
PKCS12 File Password:(confirmation)
Save
Cancel

In connection, enter the name for this remote connection, RED interface and local subnet are already chosen, check “edit advanced configuration”

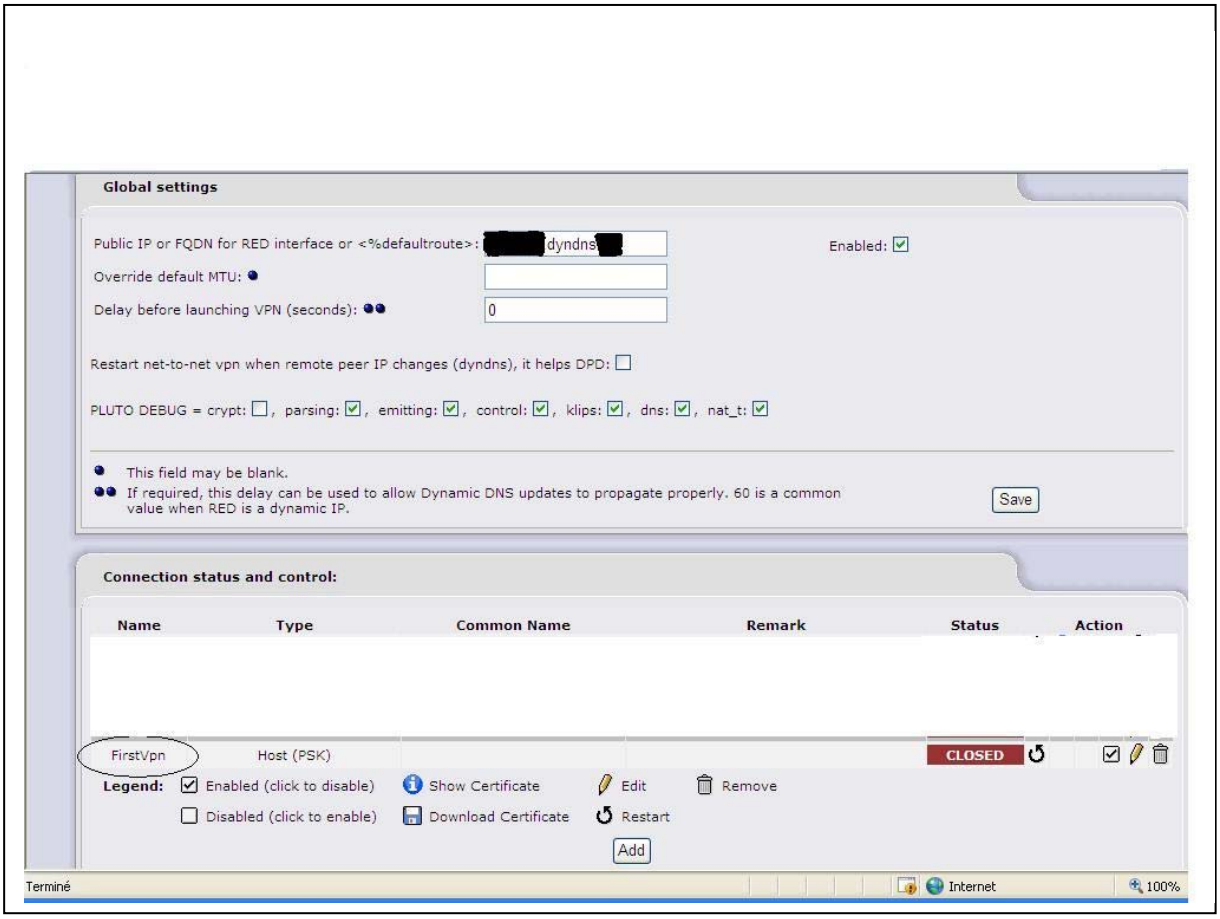
In authentication, choose “Use a Pre-Shared Key (PSK)” and enter a password that will be used in the VPNs.

Press “Save” to go on the “Advanced” settings screen:



Choose algorithms, DH group, and lifetimes for IKE and ESP and press “Save”.

Your Roadwarrior connection is now defined on VPN main screen:



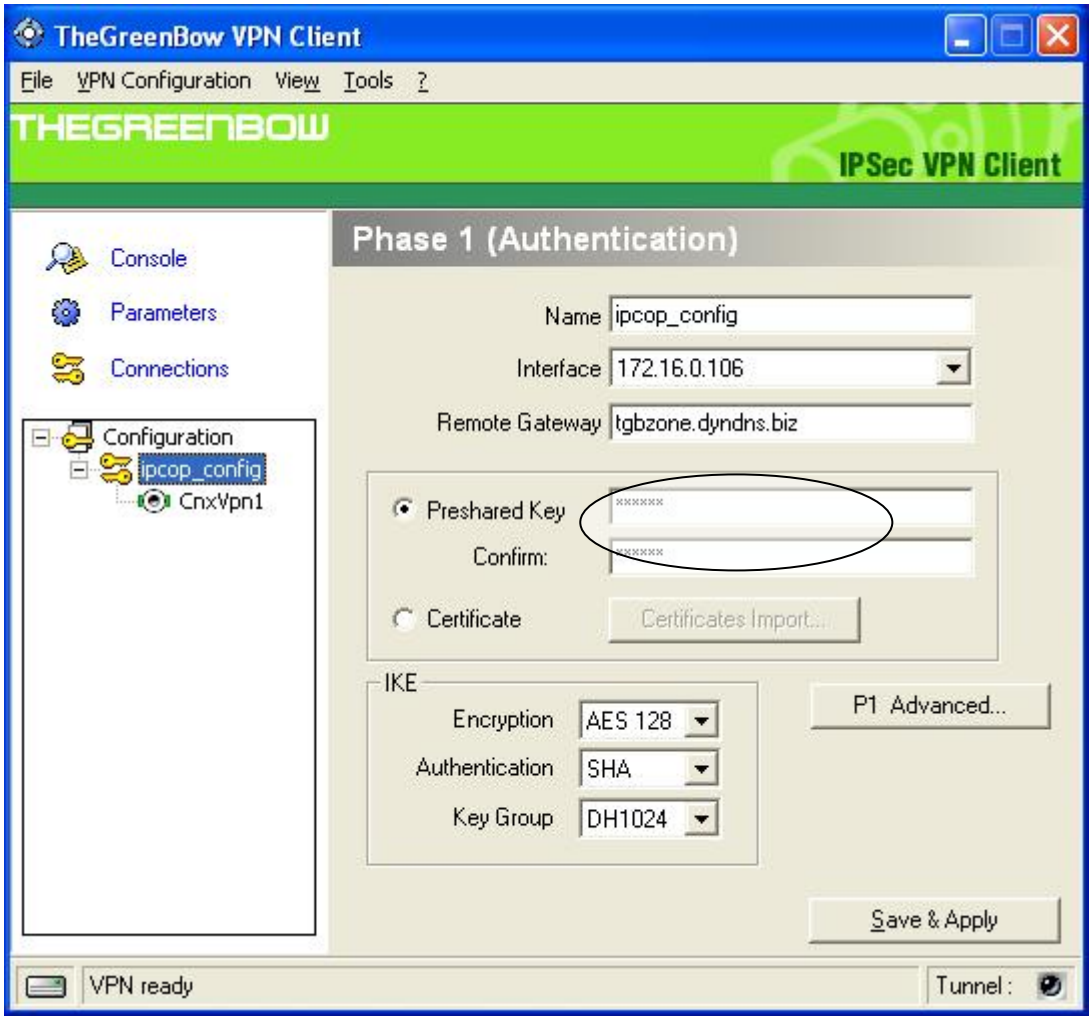
On connection status and control, click on the download certificate icon and save it (in our example it is named tgb1.p12)

IPCop VPN Configuration is finished.

3 Setting up TheGreenBow IPSec VPN Client

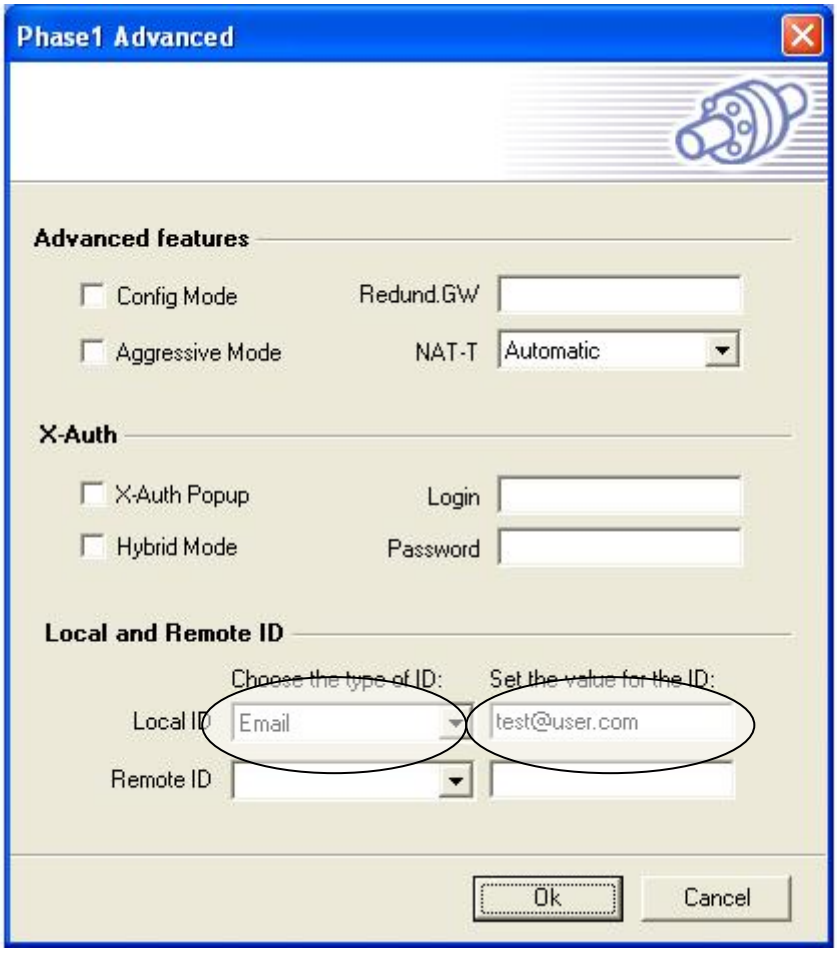
3.1 VPN Client Phase 1 Configuration

Right click on Configuration in TheGreenBow IPSec VPN Client and select "Add Phase 1".



Make sure you put in the area of Preshared Key "abcdef" as in the IPCop's config.

Choose "P1 Advanced":



Local ID can be defined as Email and depends on the type ID type defined on routers.

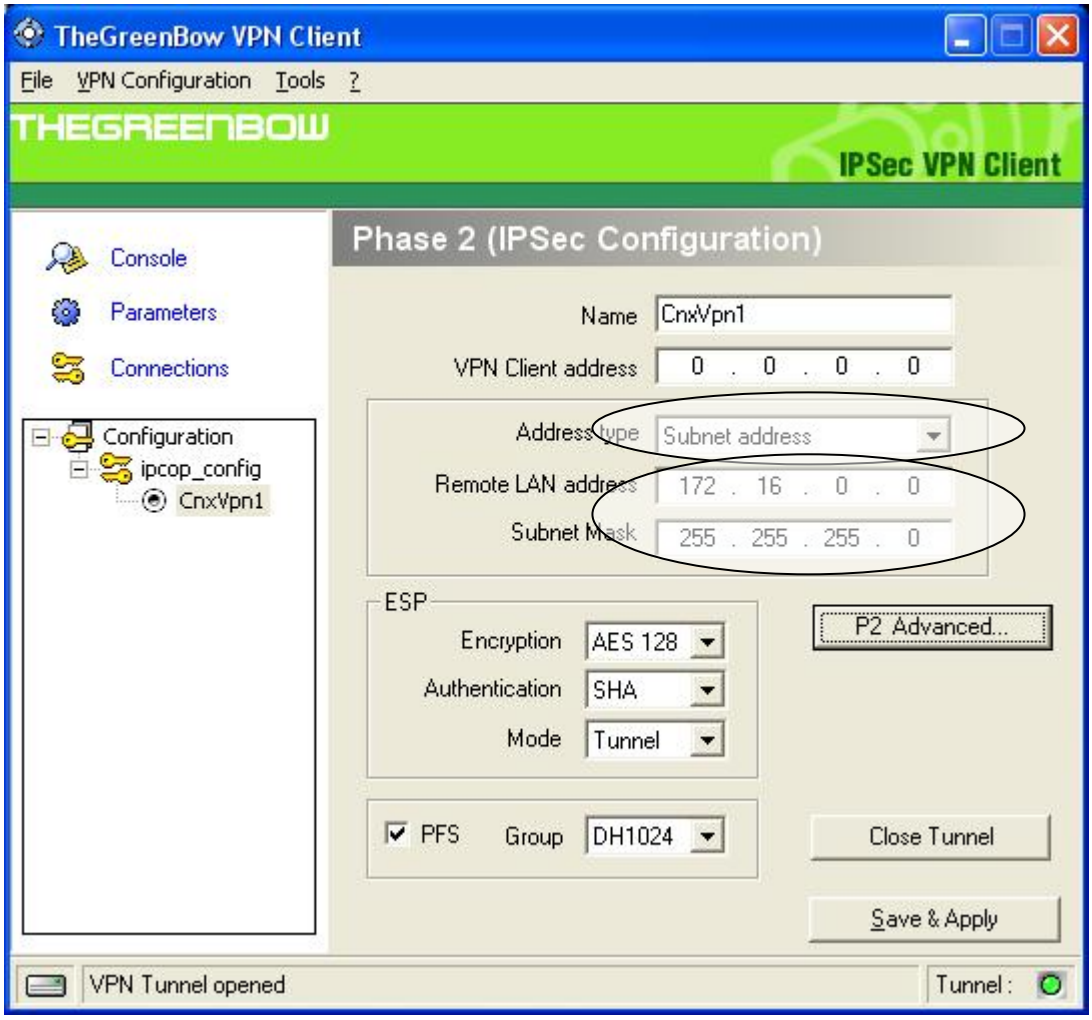
Put the Email address for the value of the ID.

Nothing is needed in Remote ID.

Press “Ok”.

3.2 VPN Client Phase 2 Configuration

Create a Phase2 by right-clicking on Phase1:



Modify Address type by choosing subnet address, and add the remote LAN address and mask (must match what was defined on IPCop)

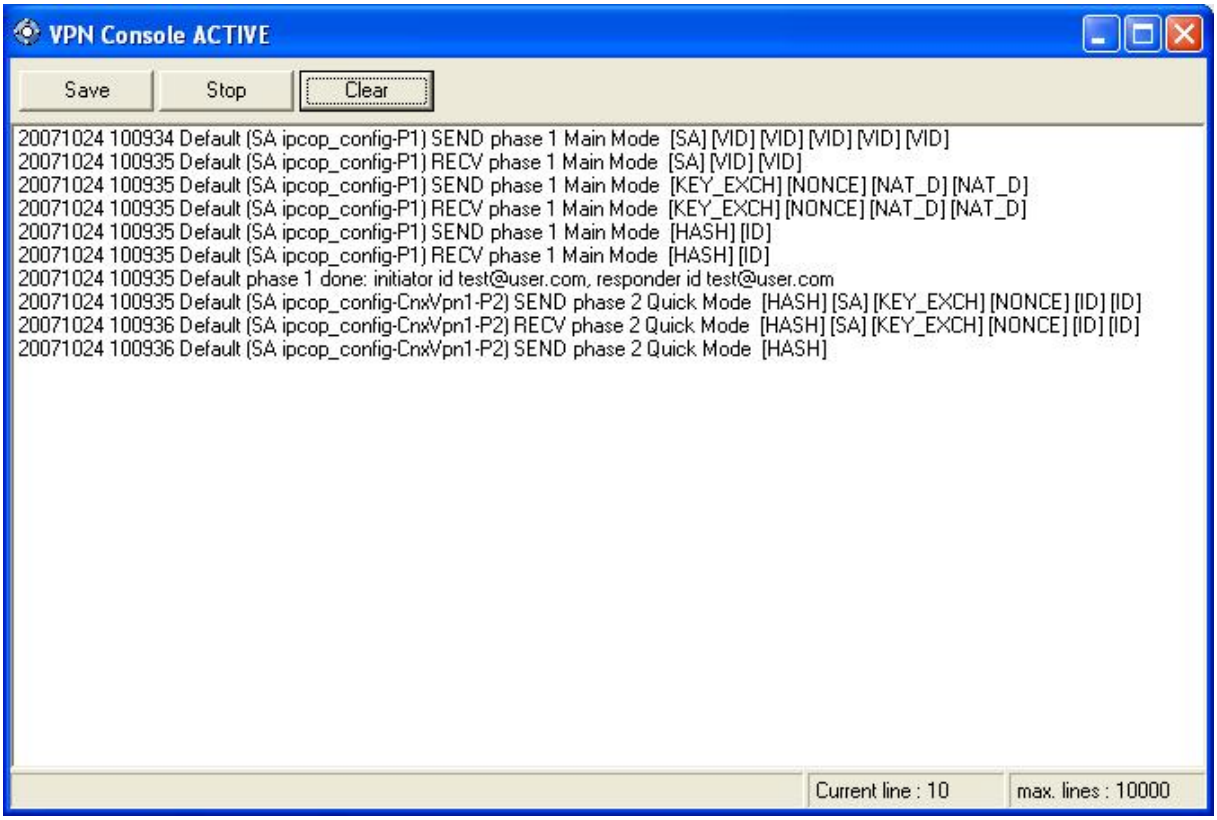
Algorithms, PFS and DH group must match IPCop settings in advanced screen in section 2.2 of this document.

The VPN Client address must not belong to the remote subnet range. In our example, we chose 0.0.0.0 meaning the VPN Client address is the physical address of the machine dynamically assigned by ISP (from a hotel for example).

If the roadwarrior tries to connect from a LAN which address is 172.16.0.0, the VPN tunnel won't establish correctly. In this case you must specify an IP address in another range (10.0.0.1 for example, or 192.168.0.1 or whatever private IP address you wish)

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.

Successful console log for this VPN tunnel:



4 Tools in case of trouble

Configuring an IPSec VPN tunnel can be a hard task. One missing parameter can prevent a VPN tunnel from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: 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 tool 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.

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 tunnel 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 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.

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