TheGreenBow IPSec VPN Client

Guide de Configuration

Resix NetxServ

Site Web: http://www.thegreenbow.com
Contact: support@thegreenbow.com

Table des Matières

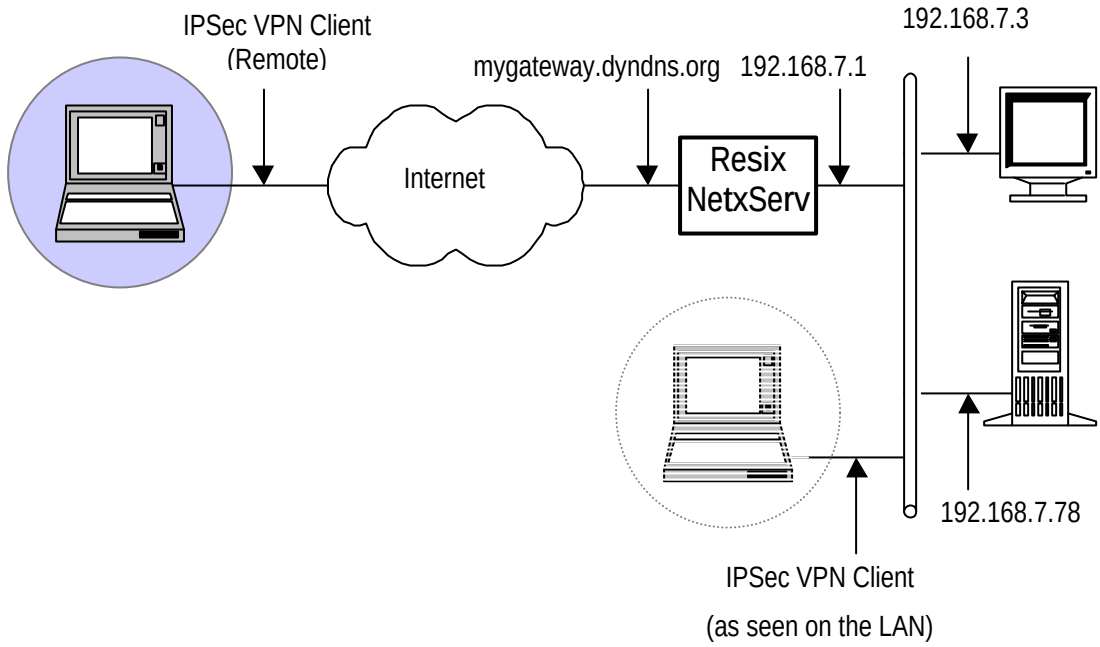
1 Introduction

1.1 But du document

Ce document décrit la configuration du Client VPN IPSec TheGreenBow avec un routeur Resix NetxServ du constructeur Resix.

1.2 Description de l'environnement réseau

Dans notre document, nous décrirons un exemple de connexion entre le client TheGreenBow VPN et le réseau local se trouvant derrière le routeur Resix NetxServ. Le client VPN est connecté à l'Internet par son FAI. Dans le réseau local, le client utilisera une adresse IP virtuelle. Toutes les adresses dans ce document sont données à titre d'exemple.



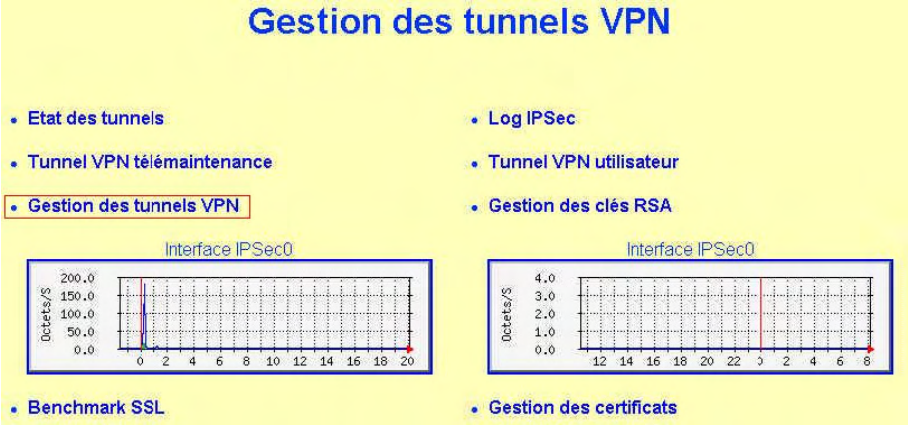
2 Configuration VPN du routeur Resix NetxServ

Cette section décrit la configuration VPN de votre Routeur VPN Resix NetxServ.

2.1 VPN Configuration

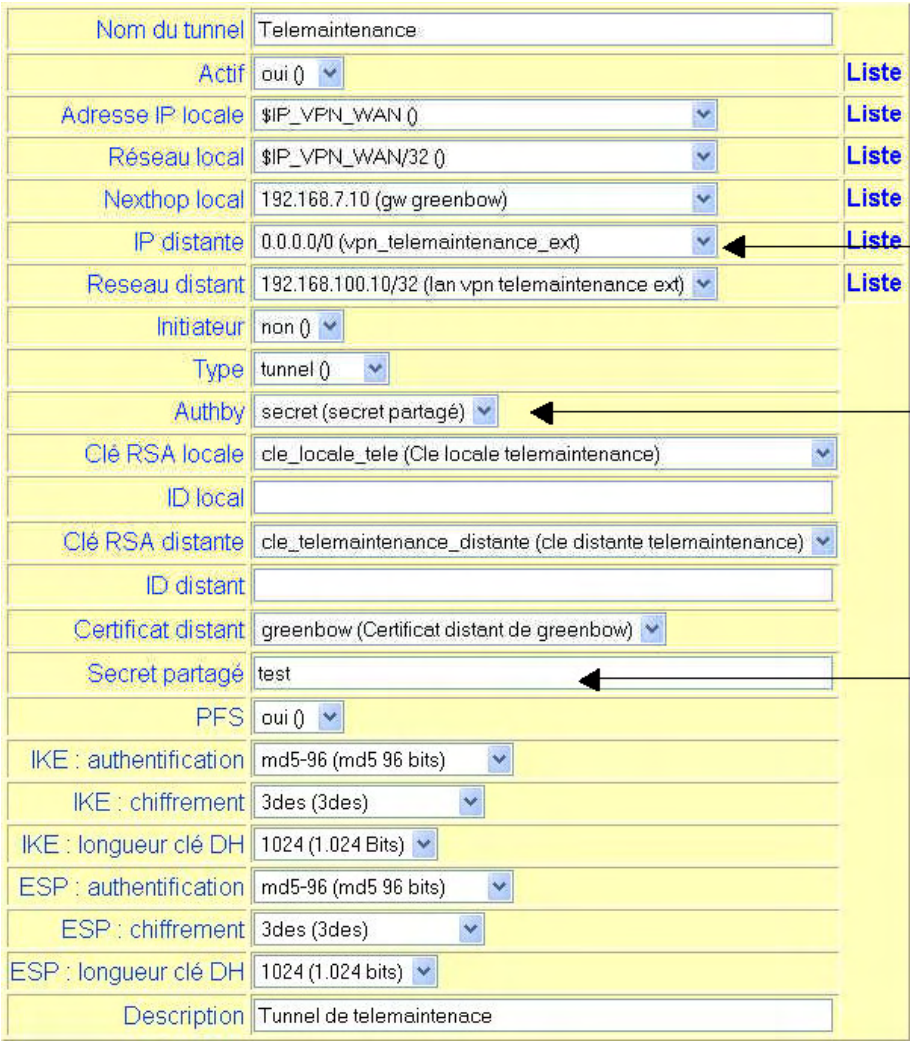
Cliquer sur l'onglet « VPN ».

Dans le menu suivant, sélectionnez: « Gestion des tunnels VPN » :



Dans l'écran suivant, remplissez les champs :

- Le secret partagé doit également être saisie dans la configuration du client IPSec TheGreenBow, en Phase 1.
- Remplir le champ IP distante par : 0.0.0.0/0



Phase 1

- IKE authentification: md5 96 bits
- IKE chiffrement: 3des
- IKE longueur clé DH: 1024 bits

Phase 2

- ESP authentification: md5 96 bits
- ESP chiffrement: 3des
- ESP longueur clé: DH 1024 bits

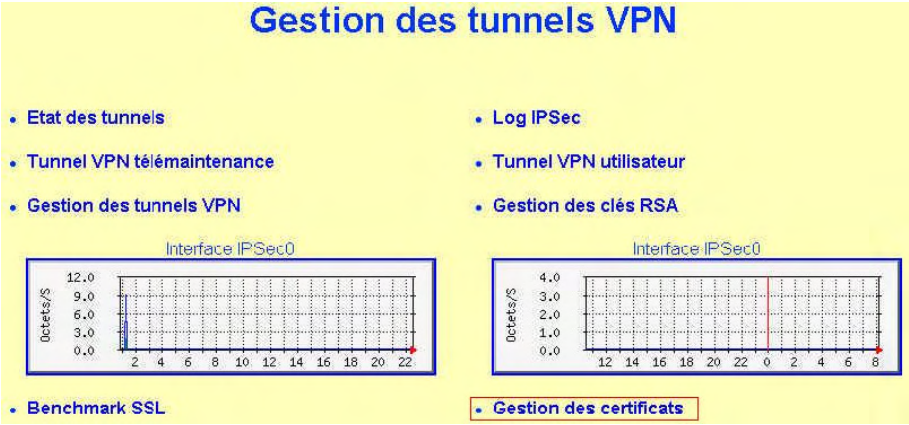
Puis, rechargez la configuration (avec ou sans reboot) en allant dans l'onglet « Action ».

2.2 Génération des certificats

Il est nécessaire de créer un certificat X.509 distant pour le Client VPN IPSec TheGreenBow

Cliquer sur l'onglet « VPN »

Dans le menu suivant, sélectionnez « Gestion des certificats » :



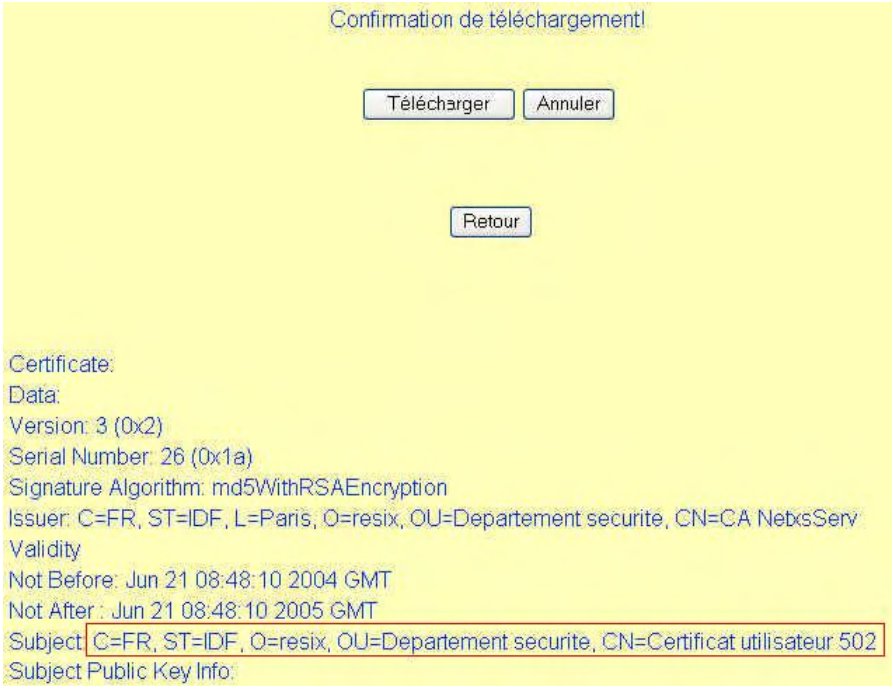
Créer un certificat distant pour le Client VPN IPSec TheGreenBow:

Numéro	Nom	Description					
0	cert_serveur	Certificat serveur	Upload	Modifier	Générer	Certificat	Clé privée
1	Greenbow	Certificat distant de greenbow	Upload	Modifier	Générer	Certificat	Clé privée

Cliquer sur le lien « **Générer** » afin de générer le certificat de TheGreenBow.

Cliquer ensuite sur les liens « **Certificat** » et « **Clé privée** » afin de télécharger respectivement le certificat (*certificat utilisateur*) et la clé privée (*clé privée utilisateur*) distante.

Copier la ligne "Subject" qui s'affiche lors de la demande de téléchargement du lien « **Certificat** » (certificat utilisateur). Cette information servira lors de la configuration du NetxServ mais aussi pour les paramètres du Client VPN TheGreenBow.



Cliquer finalement sur le lien «Clé privée » de la ligne 0 afin d'avoir le certificat d'authentification du NetxServ (certificat racine)

Transmettre ces 3 fichiers au Client VPN IPSec TheGreenBow.

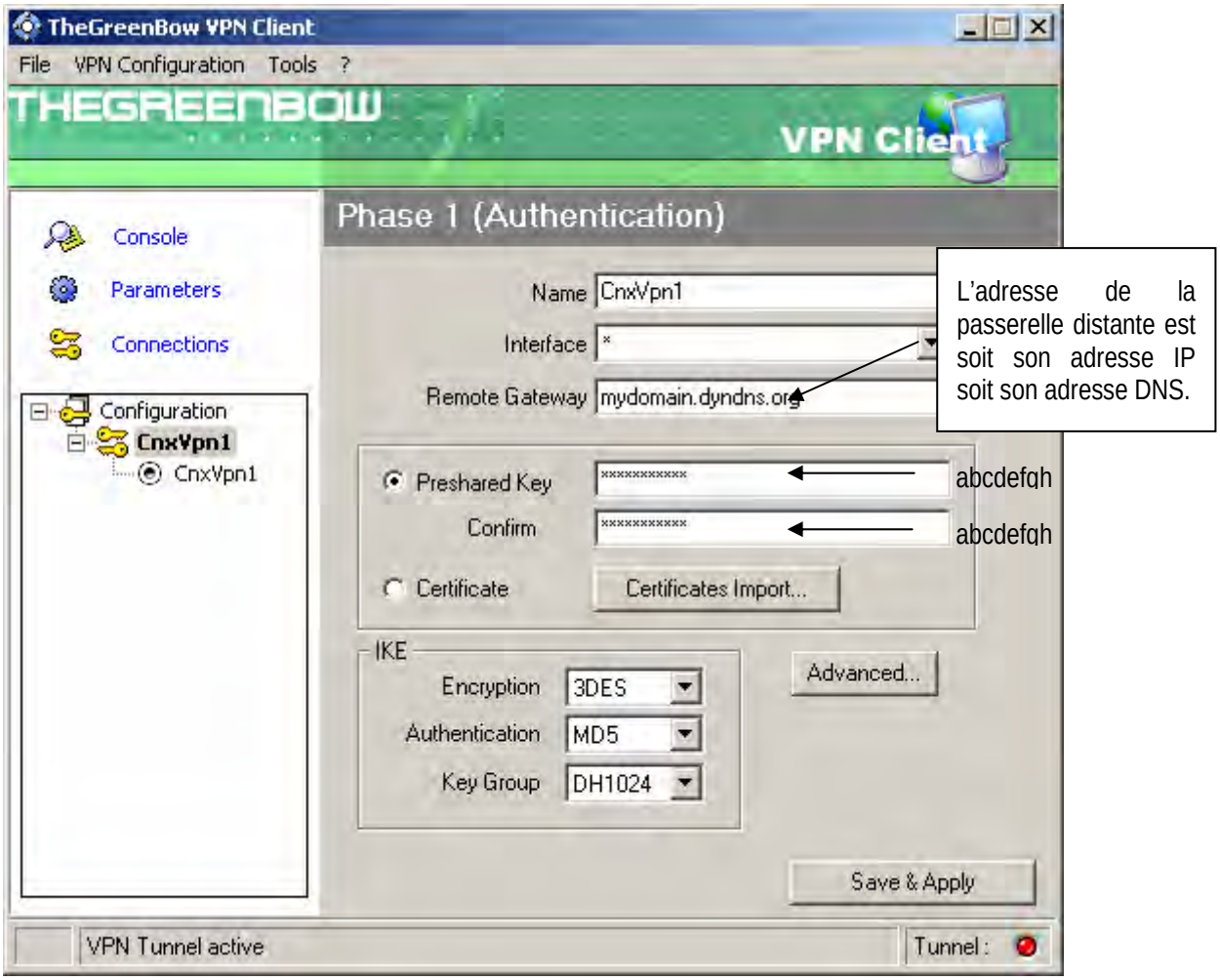
3 TheGreenBow IPSec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration

Dans le champ "Interface", vous pouvez sélectionner une étoile ("*") si le client reçoit une adresse IP dynamique de son FAI par exemple.

Dans le champ "Adresse distante", entrez l'adresse IP ou un nom DNS du routeur distant.

En cliquant sur le bouton "Avancé", vous pouvez configurer Phase 1 IDS et le Mode Agressif.

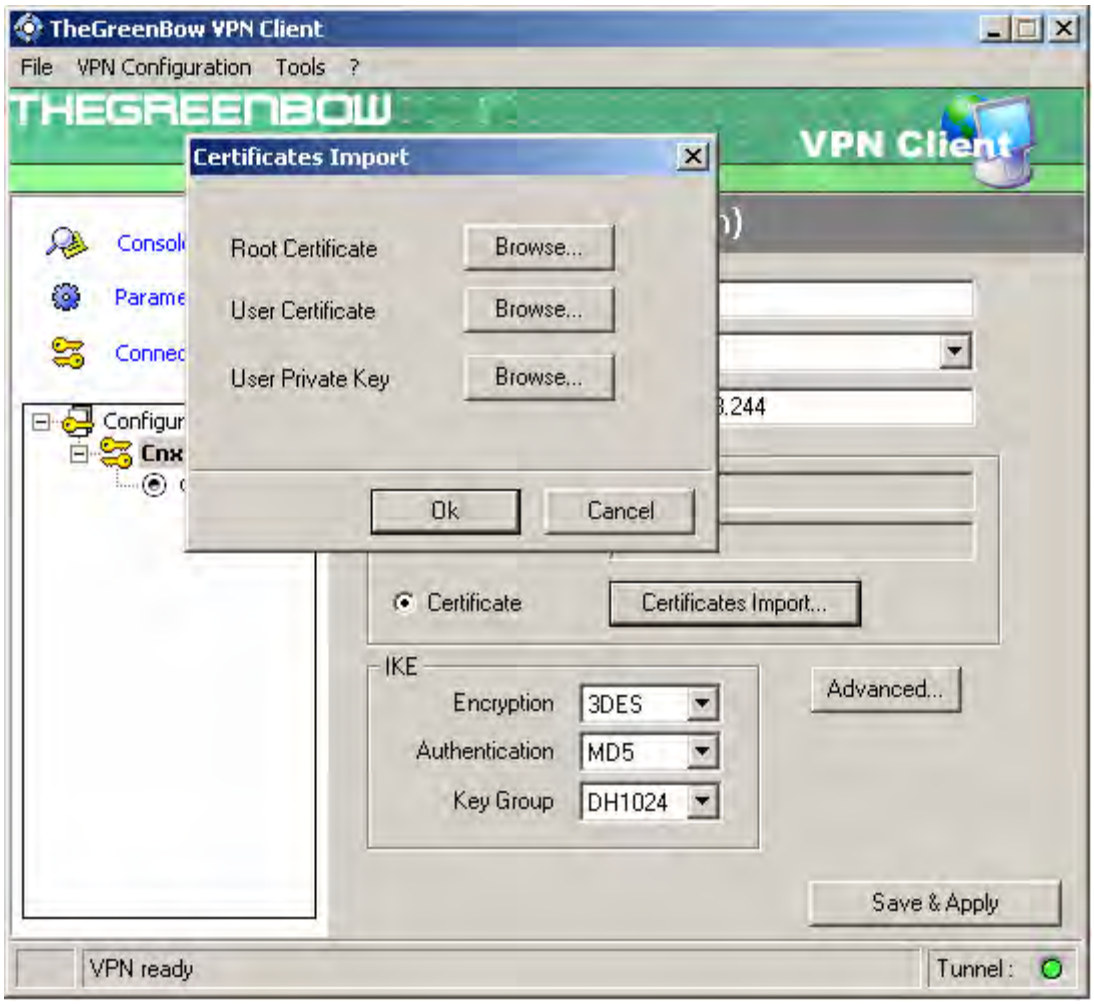


Configuration Phase 1

3.2 Import des Certificats dans le Client VPN

Cocher l'option "Importer Certificats ..."

Importer ensuite les certificats crées à l'aide du NetxServ.



Import Certificat

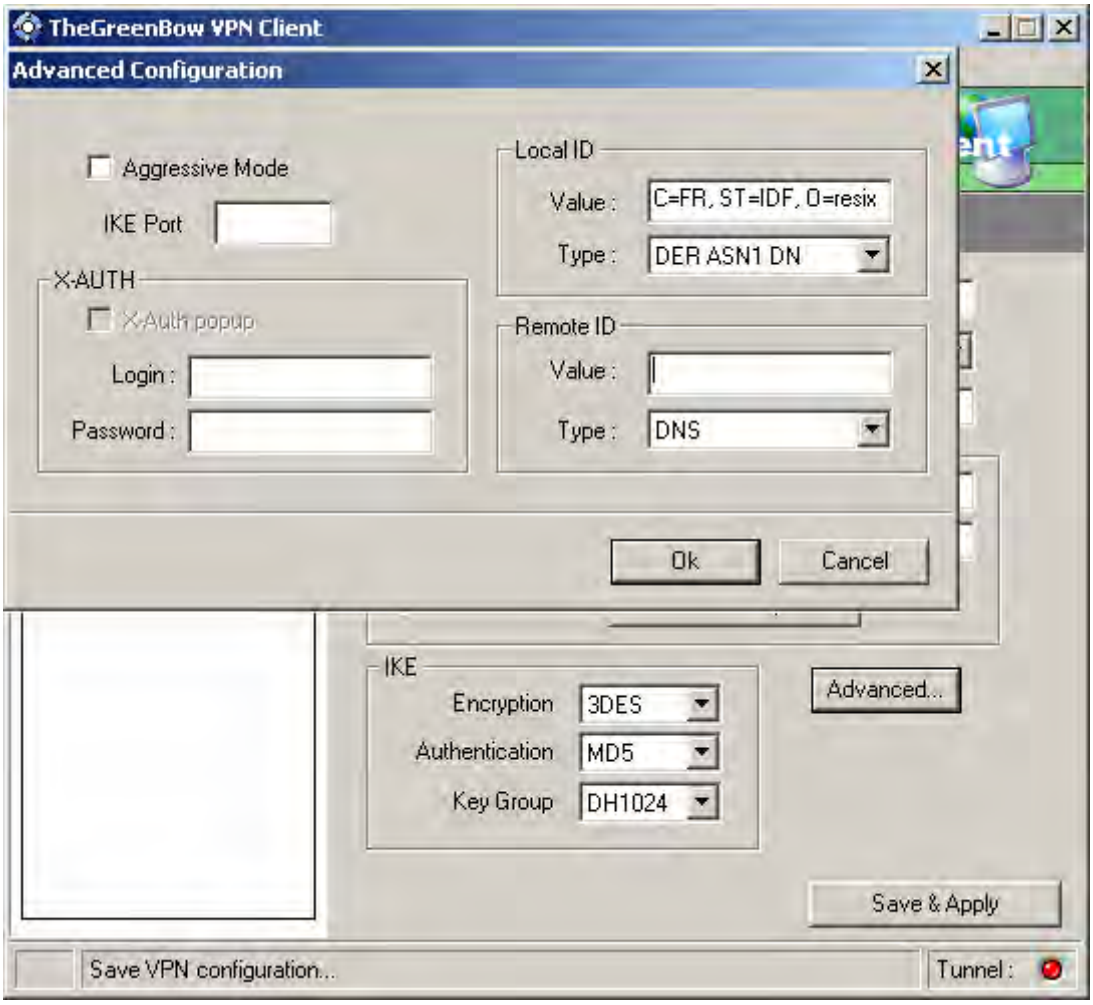
3.3 Configuration Certificat Local ID

Cliquer sur le bouton "Avancé" ou Avdvanced".

Pour local id choisir “DER ASN1 DN”

Pour le champ valeur remplir avec la ligne Subject copié lors du téléchargement du certificat utilisateur.

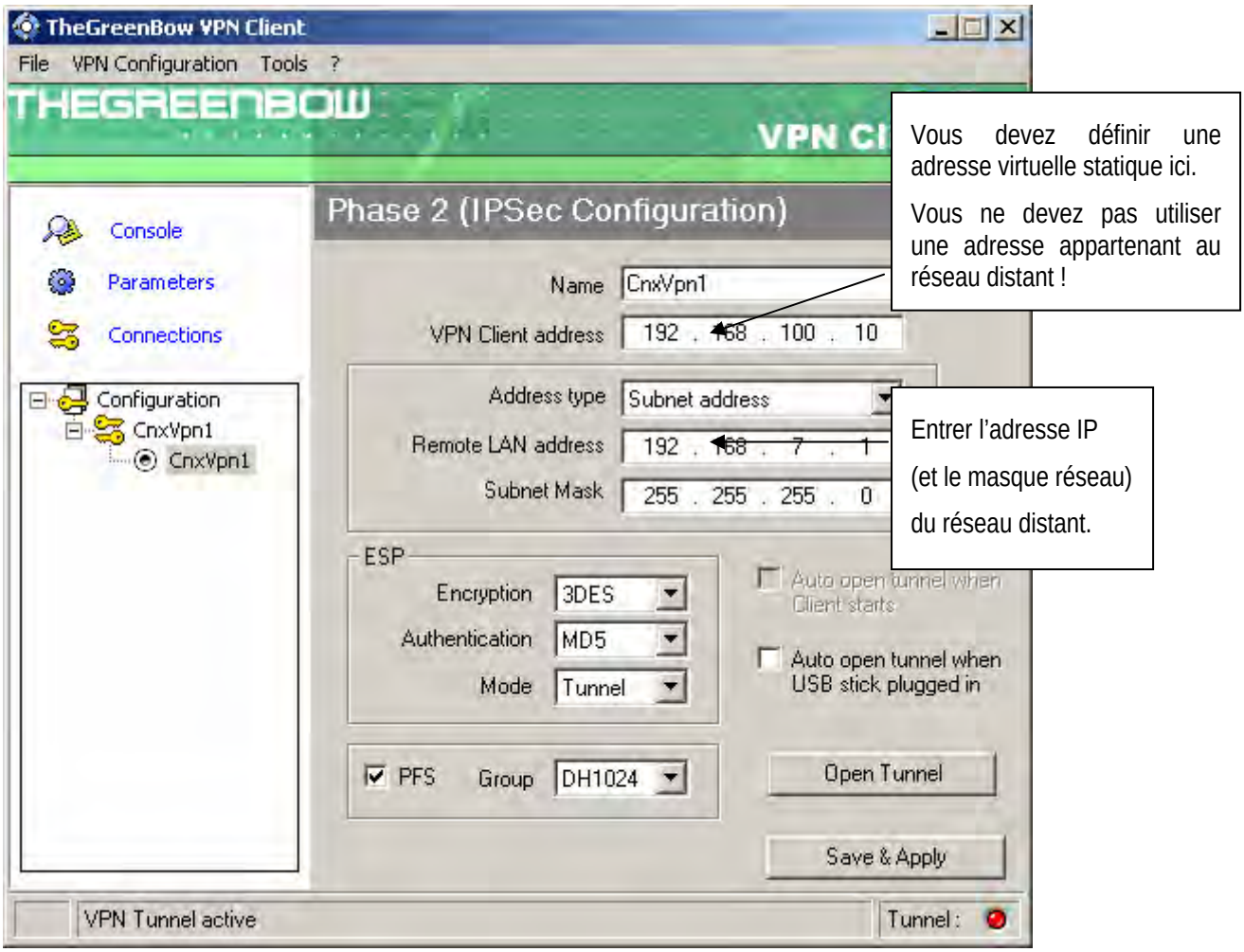
Configuration phase 1 (mode avancé)



Advanced Configuration

3.4 VPN Client Phase 2 (IPSec) Configuration

Dans cette fenêtre, vous définissez la configuration VPN IPSec.



Configuration Phase2

Le champ "Adresse Locale" est l'adresse IP virtuelle du client au sein du réseau. Cette adresse ne doit pas appartenir au réseau distant.

3.5 Ouvrir un tunnel VPN IPSec

Lorsque le Routeur VPN Resix NetxServ et le Client IPSec VPN TheGreenBow ont été configuré comme decrit precedement, you etes prêt pour établir des tunnels VPN IPSec. Soyez d'abord certain d'autoriser le traffic VPN IPSec dans votre Firewall.

1. Cliquer sur "Appliquer les Règles" pour prendre en compte les dernières modifications faites à votre configuration VPN.
2. Cliquer sur "Ouvrir le tunnel", ou genrer du trafic qui provoquera automatiquement l'ouverture de tunnels VPN IPSec (ex.: ping, IE Browser, …)
3. Cliquer sur "Connections" pour voir les tunnels VPN ouverts.
4. Cliquer sur "Console" si vous voulez accéder aux logs VPN IPSec et ajuster le niveau de filtrage et diminuer le nombre de message IPSec.

4 Contacts

Info et mise à jour sur le site web : http://www.thegreenbow.com

Support technique par email : support@thegreenbow.com

Contacts commerciaux par téléphone au +33 1 43 12 39 37 ou par email : info@thegreenbow.com