 TheGreenBow IPsec VPN Client
Guide de Configuration
BeWAN LanBooster 6104

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

Table of contents

1	Introduction	0
1.1	But du document	0
1.2	Description de l'environnement réseau	0
2	Configuration VPN du BeWAN LanBooster 6104	0
2.1	BeWan LanBooster autoriser le trafic VPN IPSec.....	0
2.2	BeWan LanBooster paramètres IKE et cryptages.....	0
2.3	BeWan LanBooster profile interconnexion réseaux	0
3	TheGreenBow IPSec VPN Client configuration	0
3.1	VPN Client Phase 1 (IKE) Configuration	0
3.2	VPN Client Phase 2 (IPSec) Configuration	0
3.3	Ouvrir un tunnel VPN IPSec.....	0
4	Contacts.....	0

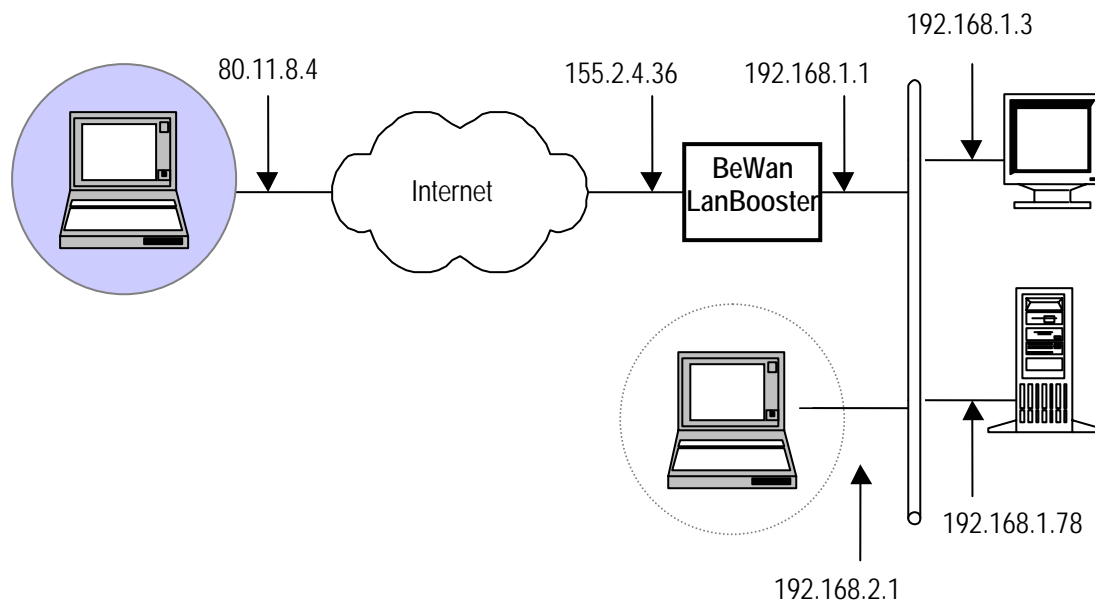
1 Introduction

1.1 But du document

Ce document décrit la configuration du Client VPN TheGreenBow avec un routeur LanBooster 6104 du constructeur BeWAN.

1.2 Description de l'environnement réseau

Dans notre document, nous décrivons un exemple de connexion entre le client TheGreenBow VPN et le réseau local se trouvant derrière le routeur BeWAN. 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 BeWAN LanBooster 6104

Cette section décrit la configuration VPN de votre Routeur VPN BeWAN LanBooster 6104. La version du firmware utilisé pour le Routeur VPN BeWAN LanBooster 6104 durant les tests était la 2.5.1 – w1.0.1 | 02/10/2004.

2.1 BeWan LanBooster autoriser le trafic VPN IPSec

Depuis le menu principal de configuration, sélectionnez "Paramétrage des accès distants et RPV (VPN)" :



BeWAN systems Configurateur Web du LanBooster 6104 xg

Menu principal
BeWAN systems

- Modèle : LanBooster 6104 xg
- Version du firmware : 2.5.1 - w1.0.1
- Date de la version : Tue Feb 10 19:45:24.66 2004
- Adresse MAC : 00-50-7F-23-98-8A

Installation Elémentaire

- >> [Paramètres administrateur](#)
- >> [Paramètres LAN TCP/IP et serveur DHCP](#)
- >> [Paramètres du réseau Wireless](#)

Installation Rapide

- >> [Accès Internet](#)

Installation Avancée

- >> [Paramétrage des plages horaires](#)
- >> [Paramétrage du NAT](#)
- >> [Paramétrage du DNS dynamique](#)
- >> [Paramétrage des routes statiques](#)
- >> [Paramétrage des accès distants et RPV \(VPN\)](#)
- >> [Paramétrage du client RADIUS](#)
- >> [Paramétrage des filtres IP et du firewall](#)
- >> [Paramétrage du service UPnP](#)
- >> [Paramétrage VLAN](#)

Administration Système

- >> [Etat de la ligne ADSL / LAN / WAN](#)
- >> [Outils de diagnostic](#)
- >> [Contrôle d'administration et agent SNMP](#)
- >> [Réglage de l'heure du routeur](#)
- >> [Réglage du syslog](#)
- >> [Etat de la connexion RPV \(VPN\)](#)
- >> [Redémarrage du système](#)
- >> [Mise à jour du firmware \(serveur TFTP\)](#)
- >> [Sauvegarde / Restauration de configuration](#)

Copyright © 2001-2004, BeWAN systems. Tous droits réservés.

Dans le menu suivant, sélectionnez "Paramétrage des modes du RPV (VPN)" :

The screenshot shows the BeWAN systems web configurator for the LanBooster 6104 xg. The breadcrumb navigation is: > Installation Avancée > Paramétrage des accès distants et RPV (VPN) << Menu principal. A central menu box contains the following options:

- >> Paramétrage du service d'appel entrant
- >> Paramétrage des modes du RPV (VPN) (highlighted with a red box)
- >> Paramétrage IKE / IPSec
- >> Paramétrage de l'appel entrant
- >> Paramétrage d'interconnexion de réseaux

Copyright © 2001-2004, BeWAN systems. Tous droits réservés.

Dans l'écran suivant, activez le mode VPN IPSec :

The screenshot shows the 'Paramètres du contrôle d'accès distant' screen in the BeWAN configurator. The breadcrumb navigation is: > Installation Avancée > Paramétrage des accès distants et RPV (VPN) << Menu principal. The screen title is 'Paramètres du contrôle d'accès distant' with a '<< Page précédente' link. Three checkboxes are present:

- Activer le service RPV (VPN) en mode PPTP
- Activer le service RPV (VPN) en mode IPSec (highlighted with a red box)
- Activer le service RPV (VPN) en mode L2TP

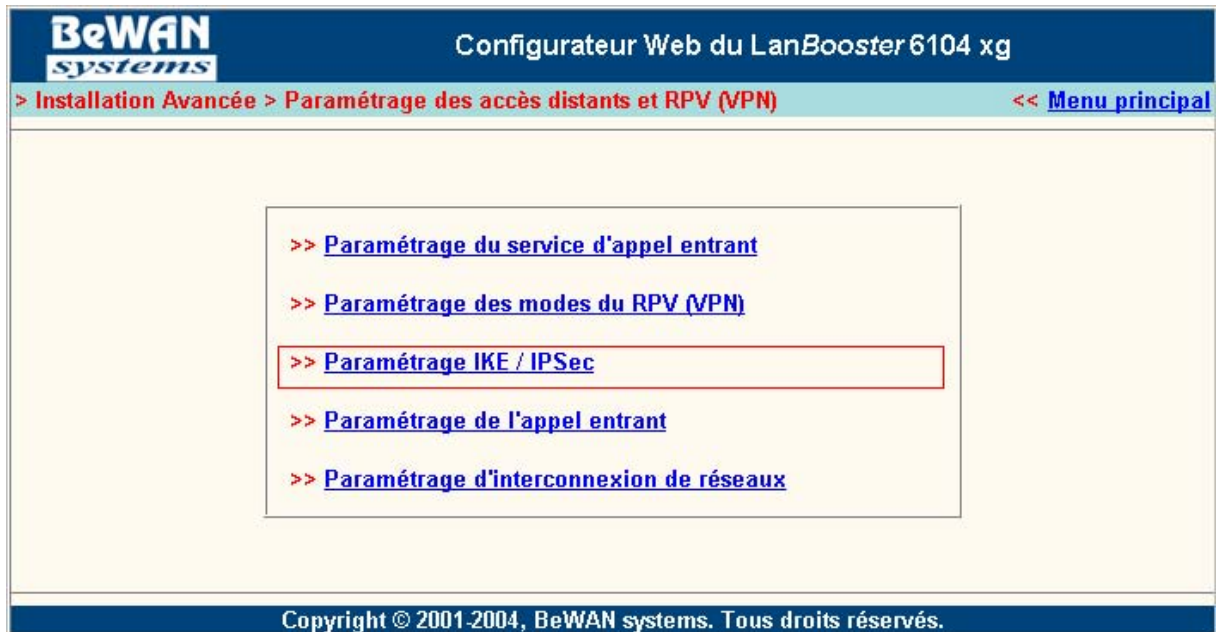
Note : Si vous essayez de faire fonctionner un serveur RPV (VPN) appartenant à votre réseau local, vous devez décocher le protocole approprié pour activer le mode transparent (pass-through) et configurer convenablement les paramètres du NAT.

OK

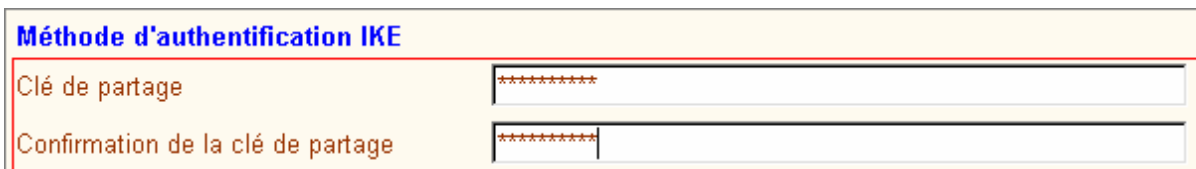
Copyright © 2001-2004, BeWAN systems. Tous droits réservés.

2.2 BeWan LanBooster paramètres IKE et cryptages

Revenez à l'écran précédent et sélectionnez "Paramétrage IKE / IPSec"

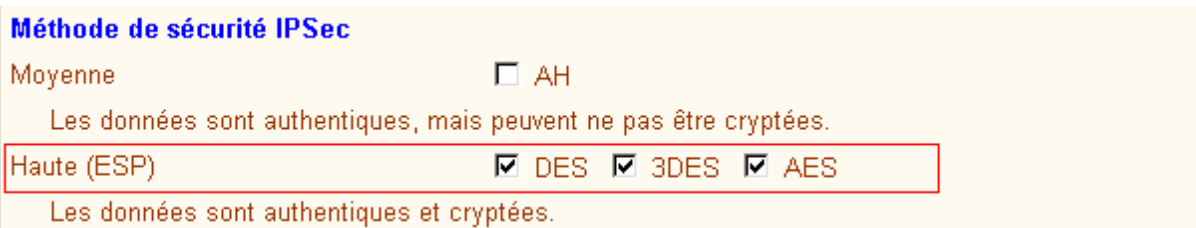


Dans l'écran suivant, remplissez le champ "Clé de partage" :



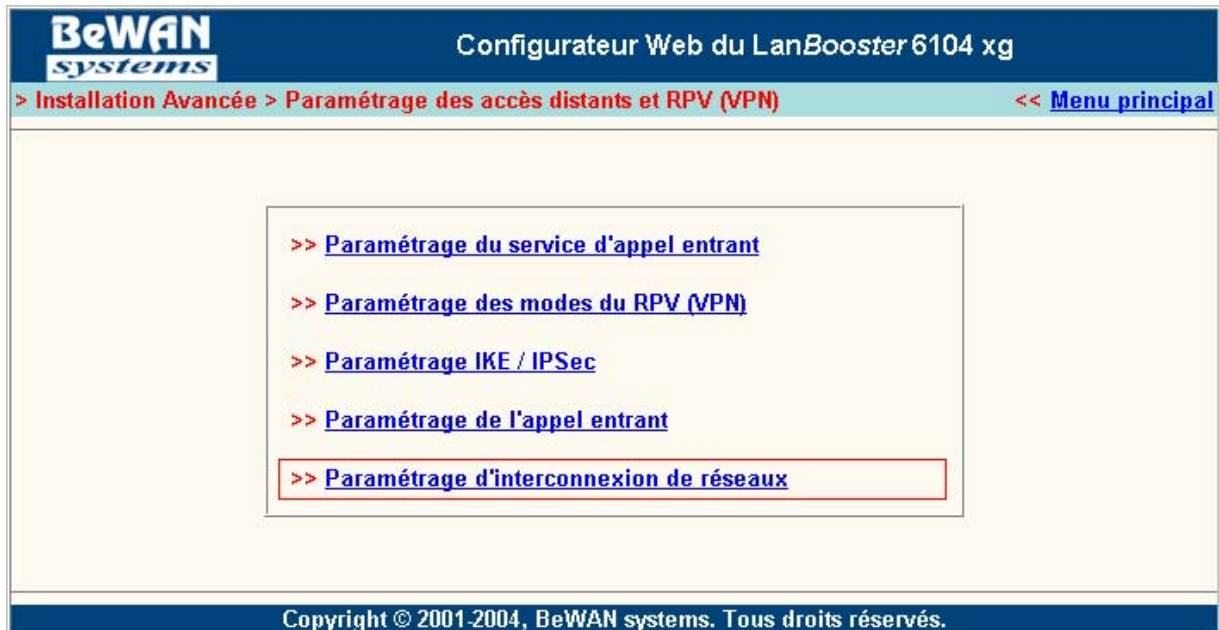
Note: Cette clé doit également être saisie dans la configuration du Client VPN IPSec TheGreenBow, en Phase 1.

Sélectionnez DES, 3DES et AES comme algorithmes pour la "Méthode de sécurité IPSec – Haute (ESP)":

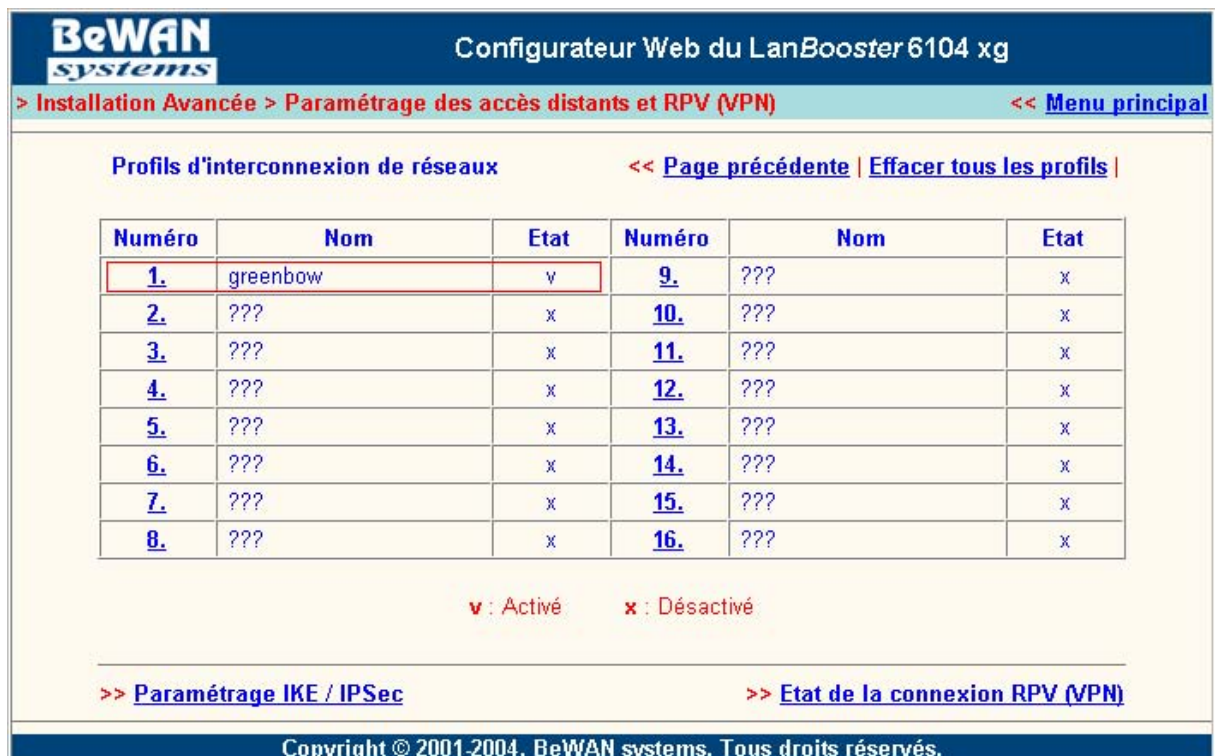


2.3 BeWan LanBooster profile interconnexion réseaux

Revenez à l'écran précédent, et sélectionnez "[Paramétrage d'interconnexion de réseaux](#)" :



Dans le menu suivant, créez une nouvelle configuration correspondant pour **chaque** poste nomade :



Numéro	Nom	Etat	Numéro	Nom	Etat
<u>1.</u>	greenbow	v	<u>9.</u>	???	x
<u>2.</u>	???	x	<u>10.</u>	???	x
<u>3.</u>	???	x	<u>11.</u>	???	x
<u>4.</u>	???	x	<u>12.</u>	???	x
<u>5.</u>	???	x	<u>13.</u>	???	x
<u>6.</u>	???	x	<u>14.</u>	???	x
<u>7.</u>	???	x	<u>15.</u>	???	x
<u>8.</u>	???	x	<u>16.</u>	???	x

v : Activé x : Désactivé

Puis, ouvrez la configuration VPN en cliquant dessus. Dans l'écran suivant, entrez les paramètres comme suit :

BeWAN
systems
Configurateur Web du LanBooster 6104 xg

> Installation Avancée > Paramétrage des accès distants et RPV (VPN)
<< Menu principal

Profil n° 1
<< Page précédente | Effacer |

1. Configuration actuelle

<input checked="" type="checkbox"/> Activer ce profil Nom du profil <input style="width: 100px;" type="text" value="greenbow"/>	Sens de l'appel <input type="radio"/> Entrant/Sortant <input checked="" type="radio"/> Entrant <input type="radio"/> Sortant <input type="checkbox"/> Rendre la connexion permanente Déconnexion si inactif depuis <input style="width: 20px;" type="text" value="0"/> seconde(s) <input type="checkbox"/> Activer le ping pour garder la connexion active Effectuer un ping sur l'IP <input style="width: 100px;" type="text"/>
--	---

2. Paramètres d'appel sortant

Type de serveur appelé <input type="radio"/> PPTP <input checked="" type="radio"/> Tunnel IPSec <input type="radio"/> L2TP avec règle IPSec <input style="width: 80px;" type="text" value="(aucune)"/> Nom d'hôte ou Adresse IP du router VPN distant (ex : monrouteur.dyndns.org ou 212.23.161.89) <input style="width: 100px;" type="text"/>	Nom d'utilisateur <input style="width: 100px;" type="text" value="???"/> Mot de passe <input style="width: 100px;" type="password"/> Authentification PPP <input style="width: 80px;" type="text" value="PAP ou CHAP"/> Compression VJ <input checked="" type="radio"/> Activée <input type="radio"/> Désactivée <hr/> Méthode de sécurité IPSec Clé de partage IKE <input style="width: 100px;" type="text" value="XXXXXXXXXXXXXXXXXXXX"/> <input type="radio"/> Moyenne (AH) <input checked="" type="radio"/> Haute (ESP) <input style="width: 80px;" type="text" value="3DES avec authentification"/> <div style="text-align: right;"><input type="button" value="Réglages avancés"/></div> <hr/> Plages horaires (1-15) <input style="width: 20px;" type="text"/> ; <input style="width: 20px;" type="text"/> ; <input style="width: 20px;" type="text"/> ; <input style="width: 20px;" type="text"/>
---	--

3. Paramètres d'appel entrant

Type d'appel entrant permis <input type="checkbox"/> PPTP <input checked="" type="checkbox"/> Tunnel IPSec <input type="checkbox"/> L2TP avec règle IPSec <input style="width: 80px;" type="text" value="(aucune)"/> <input type="checkbox"/> Activer l'authentification Adresse IP du serveur <input style="width: 100px;" type="text"/> ou ID du distant <input style="width: 100px;" type="text"/>	Nom d'utilisateur <input style="width: 100px;" type="text" value="???"/> Mot de passe <input style="width: 100px;" type="password"/> Compression VJ <input checked="" type="radio"/> Activée <input type="radio"/> Désactivée <hr/> Méthode de sécurité IPSec Clé de partage IKE <input style="width: 100px;" type="text"/> Moyenne <input type="checkbox"/> AH Haute (ESP) <input checked="" type="checkbox"/> DES <input checked="" type="checkbox"/> 3DES <input checked="" type="checkbox"/> AES
---	---

4. Paramètres TCP/IP de l'interconnexion de réseaux

Mon adresse IP WAN <input style="width: 100px;" type="text" value="0.0.0.0"/> Adresse IP de la passerelle distante <input style="width: 100px;" type="text" value="0.0.0.0"/> Adresse IP du réseau distant <input style="width: 100px;" type="text" value="192.168.2.1"/> Masque de sous-réseau du réseau distant <input style="width: 100px;" type="text" value="255.255.255.255"/> <div style="text-align: right;"><input type="button" value="Ajouter"/></div>	Direction du RIP <input style="width: 80px;" type="text" value="TX/RX"/> Version du RIP <input style="width: 80px;" type="text" value="Ver. 2"/> NAT : IP publique <input style="width: 80px;" type="text" value="Adresse IP privée"/> Routage : IP privée <input type="checkbox"/> Redéfinir ce tunnel comme route par défaut
---	--

Copyright © 2001-2004, BeWAN systems. Tous droits réservés.

Dans la section 4 (Paramètres TCP/IP), vous devez **impérativement** saisir un masque de sous – réseau de 255.255.255.255 :

4. Paramètres TCP/IP de l'interconnexion de réseaux

Mon adresse IP WAN	0.0.0.0
Adresse IP de la passerelle distante	0.0.0.0
Adresse IP du réseau distant	192.168.2.1
Masque de sous-réseau du réseau distant	255.255.255.255

Ajouter

L'adresse IP du réseau distant doit correspondre à l'adresse IP locale du Client VPN IPsec TheGreenBow au niveau de la configuration de la phase 2.

Dans la deuxième partie des paramètres TCP/IP, choisissez "**Adresse privée**".

Direction du RIP	TX/RX
Version du RIP	Ver. 2
NAT : IP publique Routage : IP privée	Adresse IP privée

Redéfinir ce tunnel comme route par défaut

Cliquez sur "OK".

Remarque : Pour chaque poste nomade utilisant le Client VPN IPsec TheGreenBow, il faut lui attribuer un profil d'interconnexion de réseaux. Tous les profils peuvent être identiques avec pour seul changement les adresses IP du réseau distant qui doivent être différentes.

Par exemple :

Poste 1 : 192.168.2.1 / 255.255.255.255

Poste 2 : 192.168.2.2 / 255.255.255.255

Poste 3 ...

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.

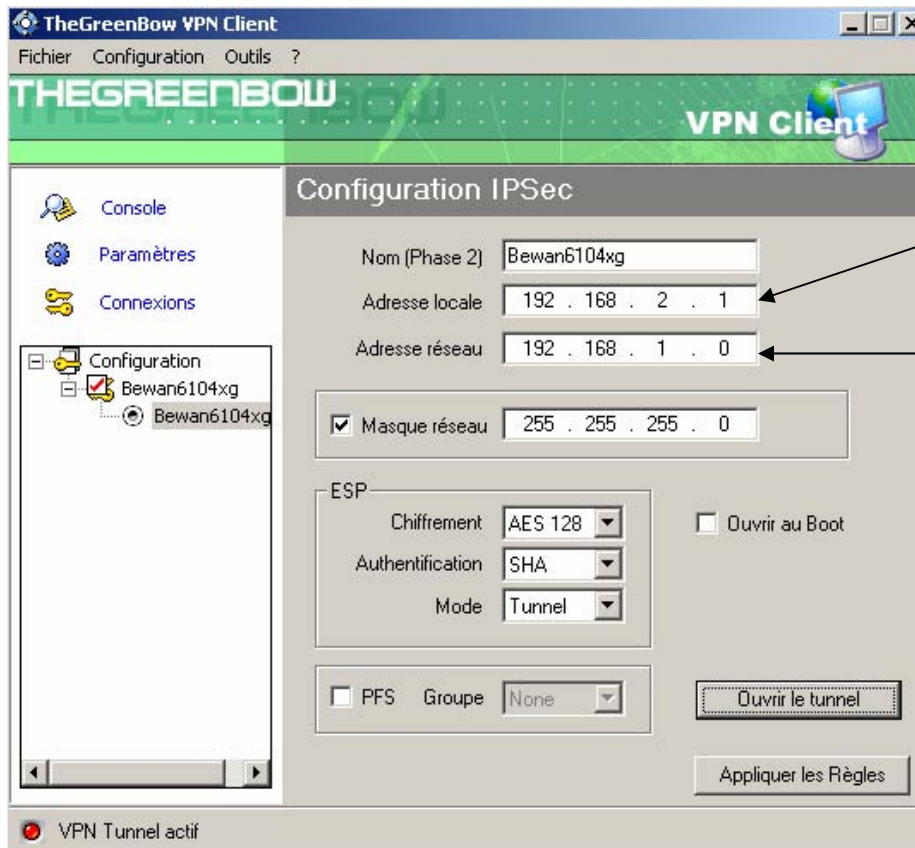
The screenshot shows the 'Authentification' configuration window in TheGreenBow VPN Client. The 'Interface' dropdown is set to '*', and the 'Adresse distante' field contains 'mydomain.dyndns.org'. The 'Clé Partagée' section has two input fields, both containing 'abcdefah'. The 'IKE' section shows 'Chiffrement' set to '3DES', 'Authentification' set to 'SHA', and 'Groupe de clé' set to 'DH768'. A callout box points to the 'Adresse distante' field with the text: 'L'adresse de la passerelle distante est soit son adresse IP soit son adresse DNS.' Another callout points to the 'Clé Partagée' fields with the text: 'abcdefah'.

Configuration Phase 1

3.2 VPN Client Phase 2 (IPSec) Configuration

Dans cette fenêtre, vous définissez la configuration VPN IPSec.

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



Vous devez définir une adresse virtuelle statique ici.

Vous ne devez pas utiliser une adresse appartenant au réseau distant !

Entrer l'adresse IP
(et le masque réseau)
du réseau distant.

Configuration Phase2

3.3 Ouvrir un tunnel VPN IPSec

Lorsque le Routeur VPN BeWAN LanBooster 6104 et le Client IPSec VPN TheGreenBow ont été configuré comme décrit précédemment, vous êtes prêt pour établir des tunnels VPN IPSec. Soyez d'abord certain d'autoriser le trafic 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 générer 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 (0)1 43 12 39 37 ou par email : info@thegreenbow.com