TheGreenBow IPSec VPN Client

Guide de Configuration

Arkoon
Security Appliances

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

Table des Matières

1 Introduction 0
1.1 But du document 0
1.2 Description de l'environnement réseau 0
2 Configuration VPN du routeur Arkoon 0
2.1 Création d'un Certificat 0
2.2 Création d'un utilisateur 0
2.3 Activation du Module VPN 0
2.4 Paramétrage du VPN 0
2.5 Définition des entités extrêmes du tunnel VPN 0
2.6 Définition des algorithmes IKE et ESP 0
2.7 Création d'une règle de flux 0
2.8 Définition du chiffrement par VPN 0
3 TheGreenBow IPSec VPN Client configuration 0
3.1 VPN Client Phase 1 (IKE) Configuration 0
3.2 Certificat Local ID Configuration 0
3.3 VPN Client Phase 2 (IPSec) Configuration 0
3.4 Ouvrir un tunnel VPN IPSec 0
4 Contacts 0

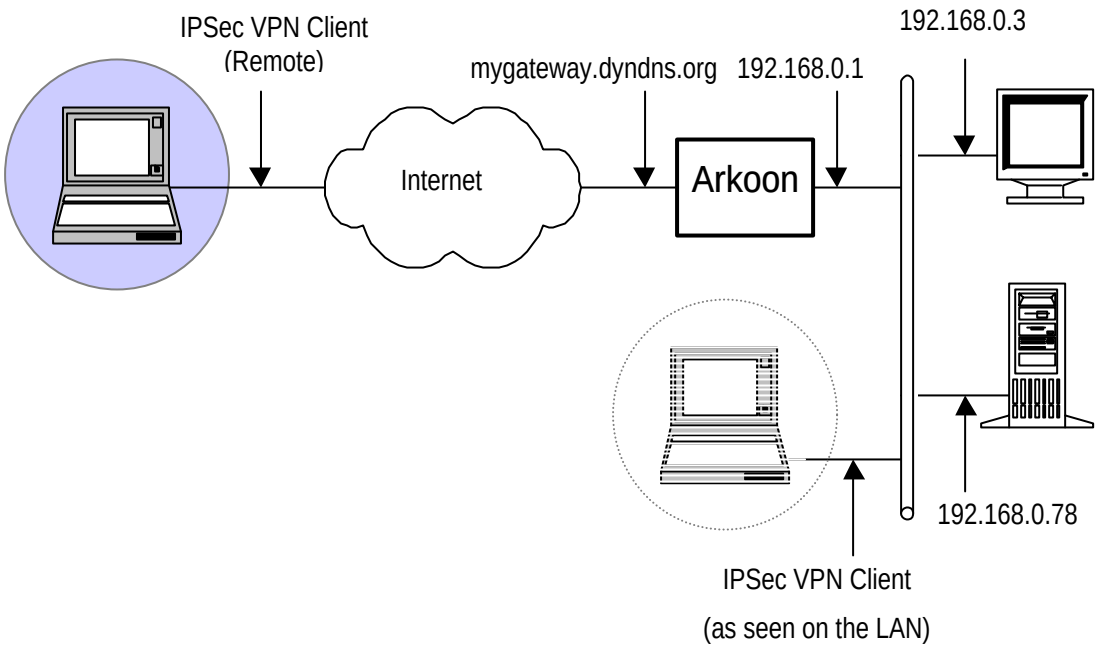
1 Introduction

1.1 But du document

Ce document décrit la configuration du Client VPN TheGreenBow avec un routeur Arkoon Security Appliances A Series du constructeur Arkoon.

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 Arkoon. 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.



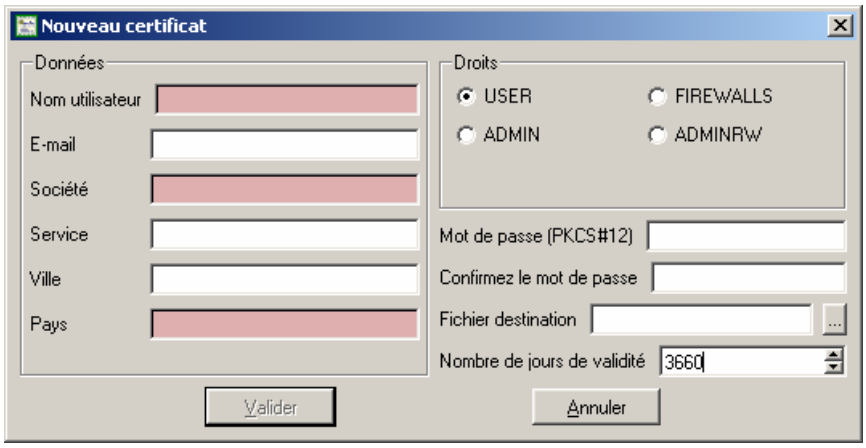
2 Configuration VPN du routeur Arkoon

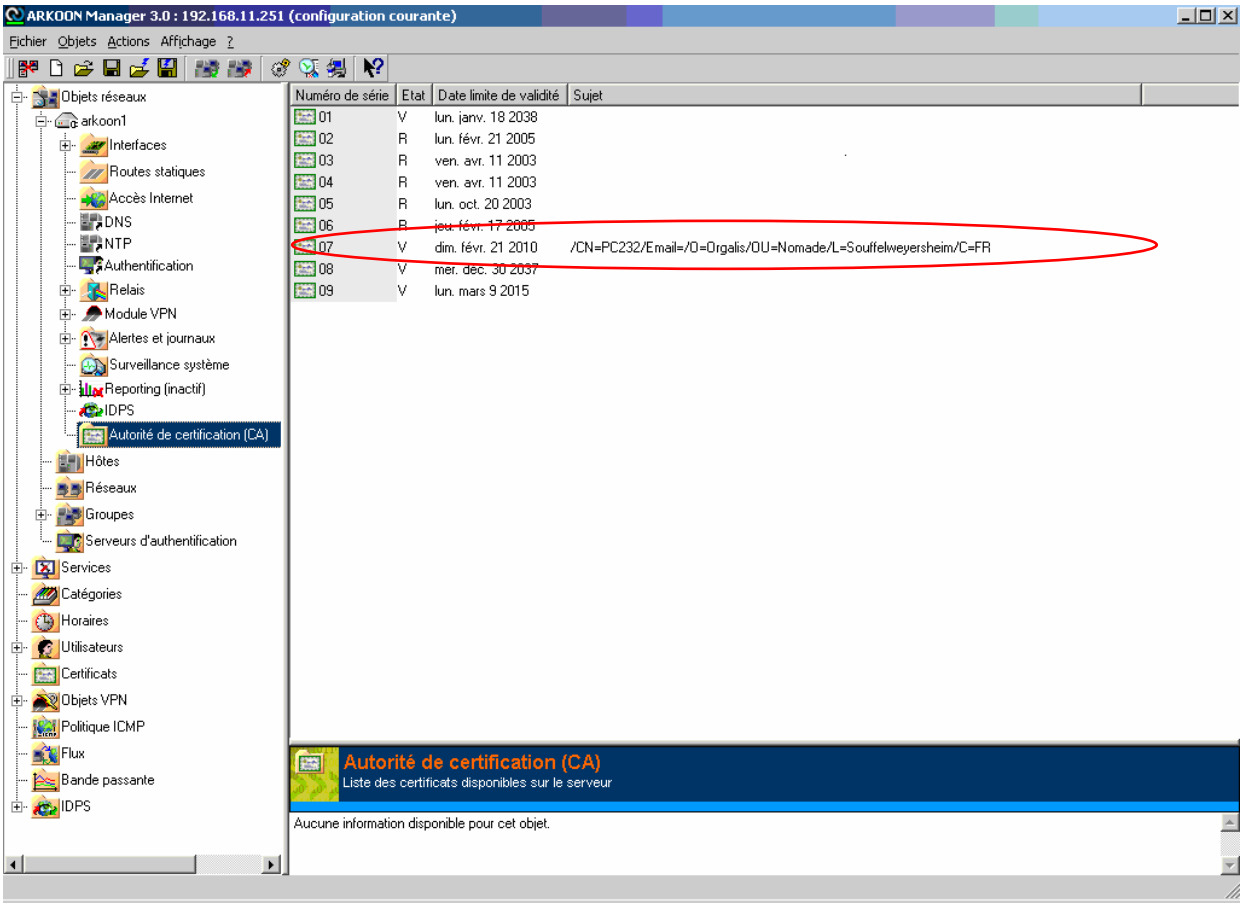
Cette section décrit la configuration VPN de votre Routeur VPN Arkoon.

2.1 Création d'un Certificat

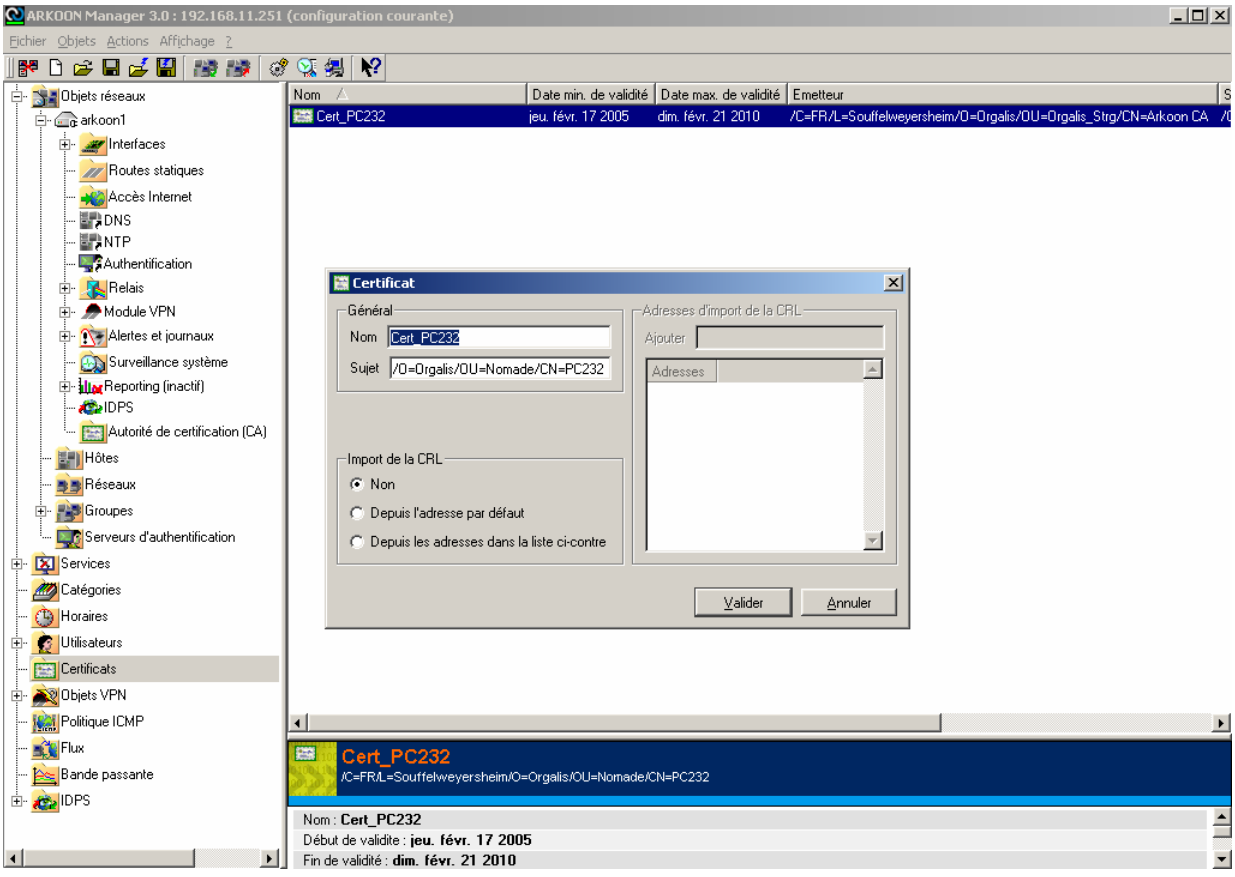
Dans l'Autorité de Certification, créer un nouveau certificat de type « User » avec les caractéristiques suivantes:

- Renseigner les zones Nom d'utilisateur, E-mail (optionnel), Société, Service, Ville, Pays (=FR)
- Spécifier le mot de passe ;
- Spécifier le chemin et le nom du fichier générer
- Définir la durée de validité du certificat



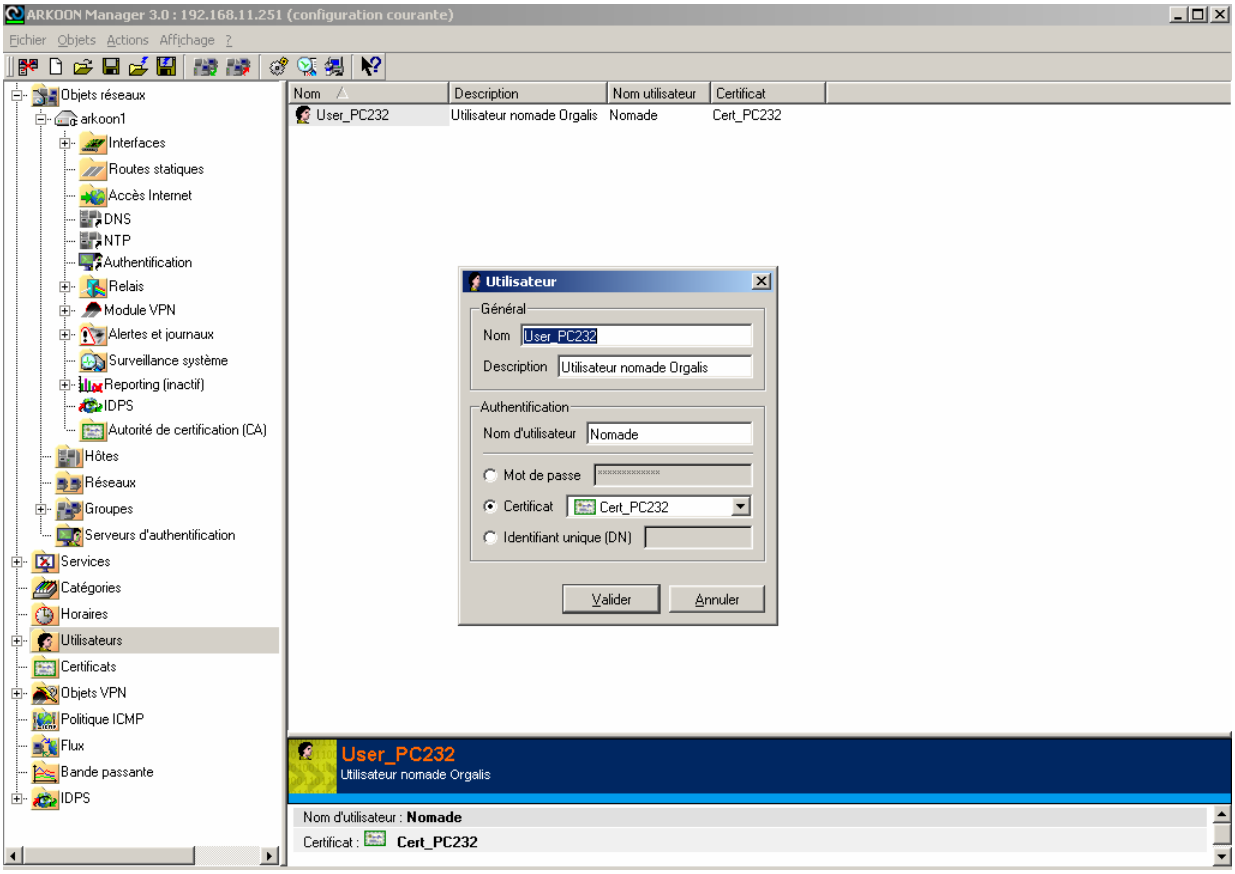


Dans les certificats (utilisés), associer le certificat précédemment créé dans la CA à un objet utilisé



2.2 Création d'un utilisateur

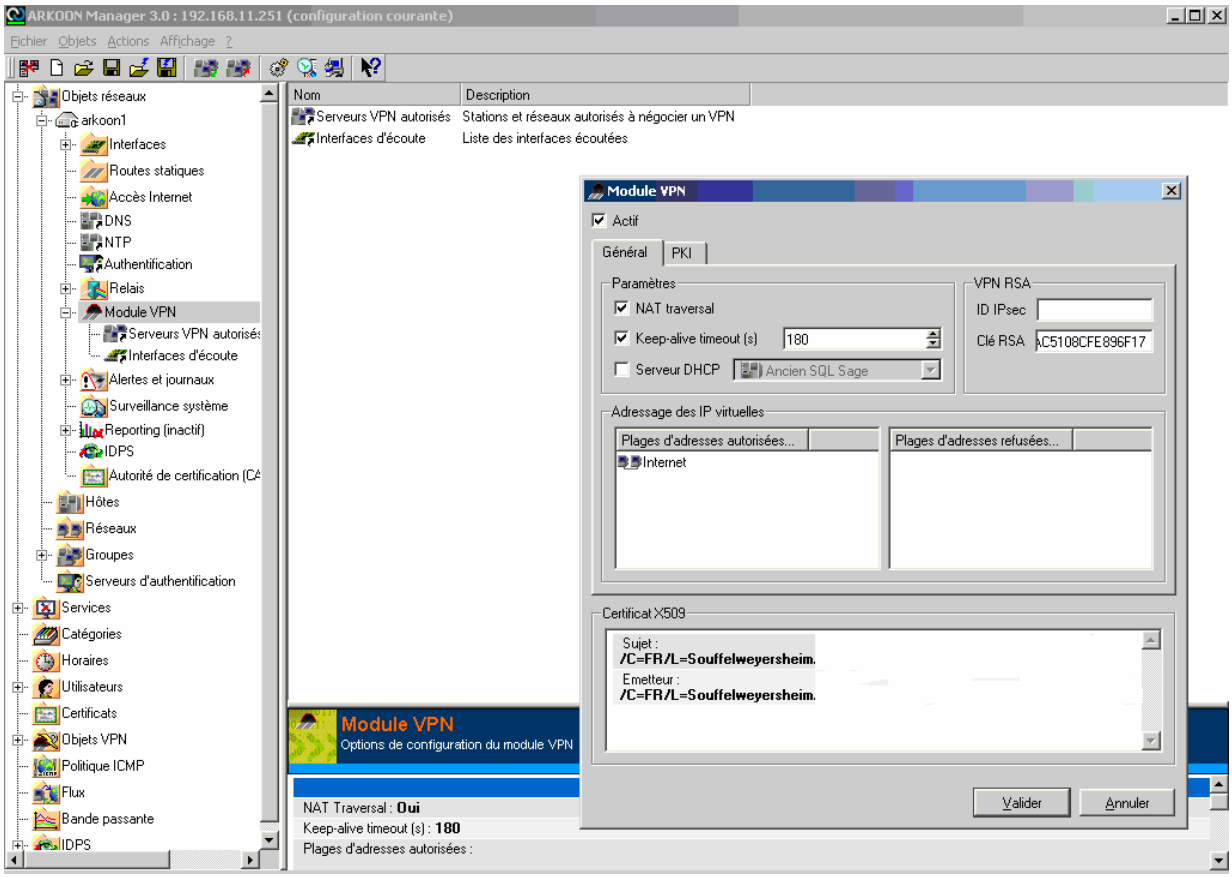
Créer un utilisateur et indiquer qu'il utilise le certificat créé à l'étape précédente (nom d'utilisateur = quelconque)

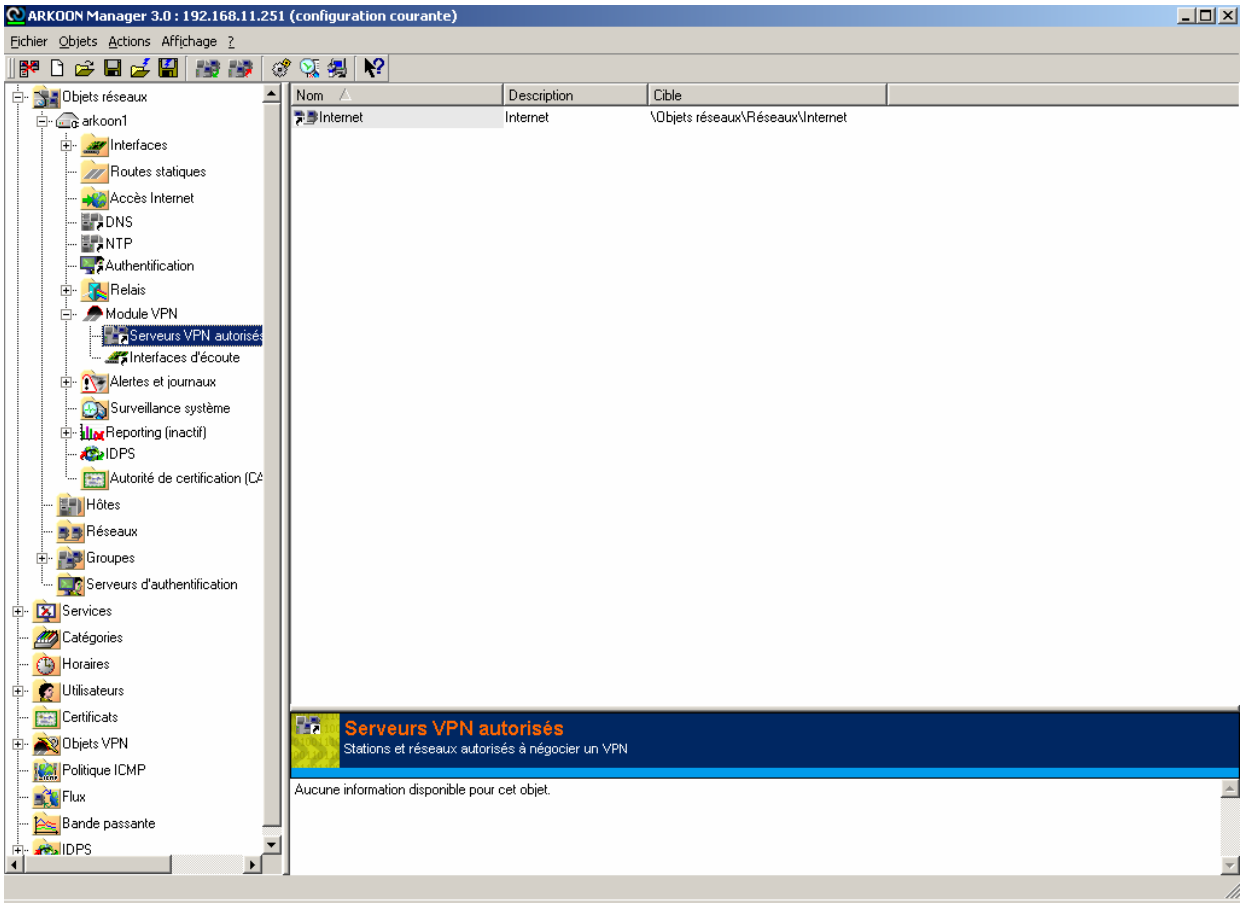


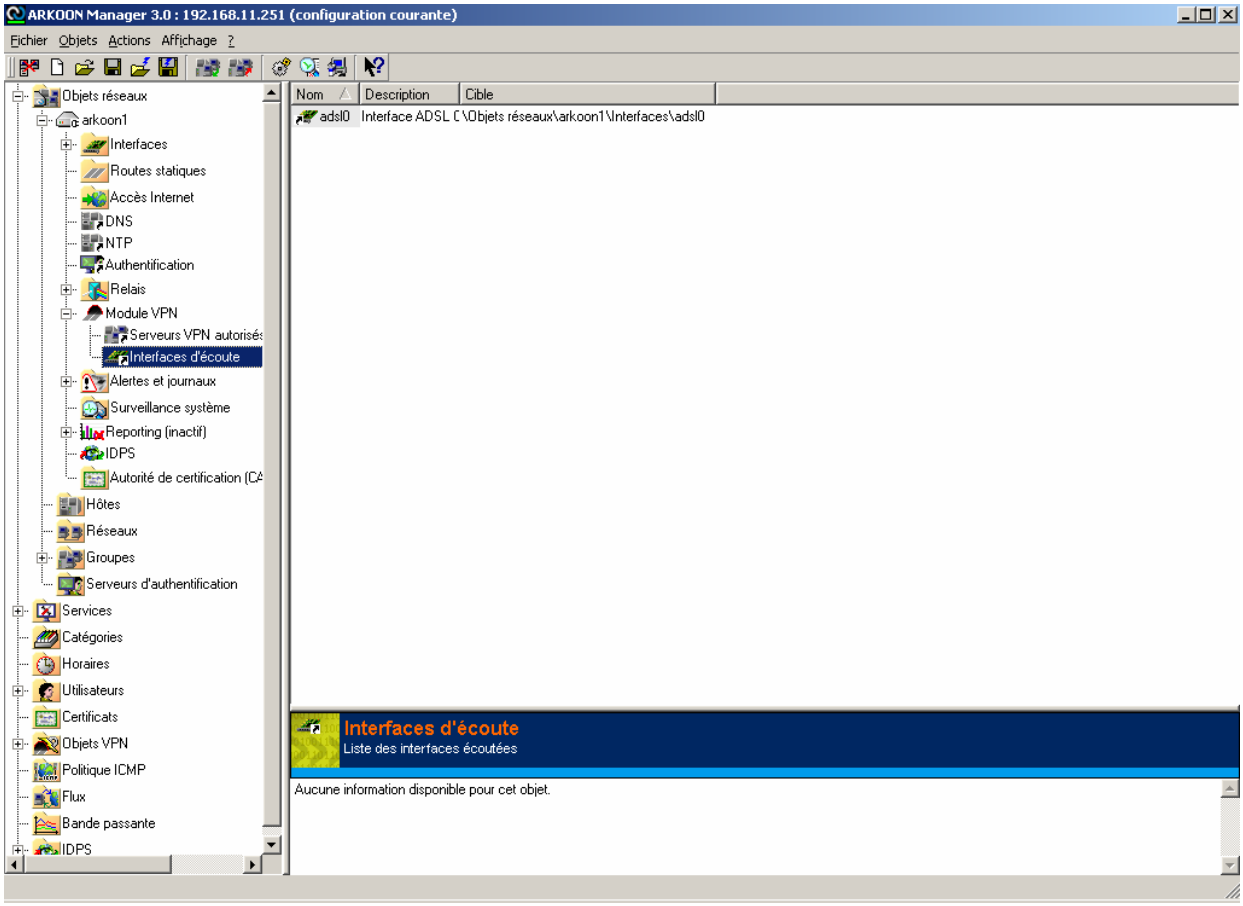
2.3 Activation du Module VPN

Si cela n'a pas déjà été fait, activer le "module VPN" ; si nécessaire cocher NAT-Traversal et définir le « Keep alive timeout ».

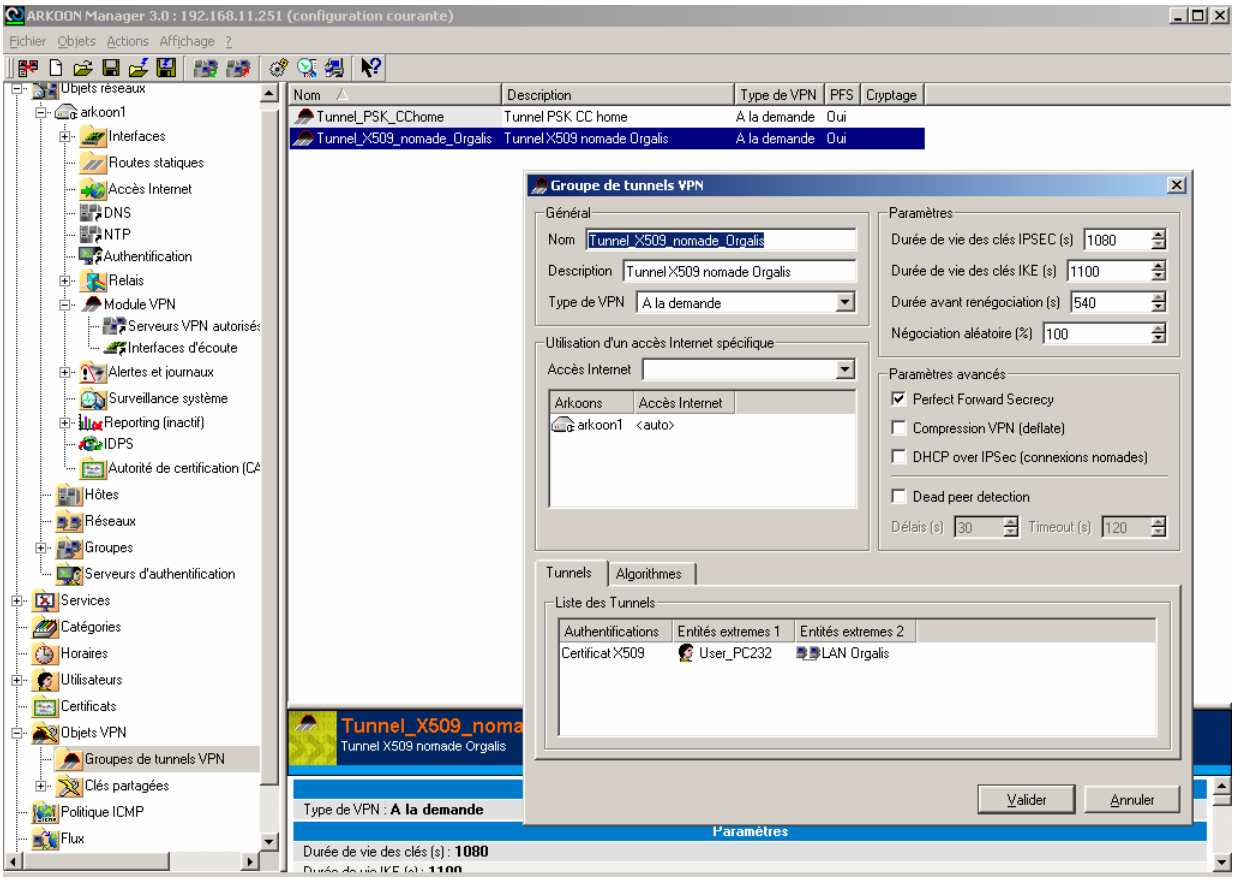
Plage d'adresses autorisées = IP virtuelles ; si ces IP sont connues et bien définies, les paramétrer, sinon autoriser toutes adresses IP (Internet)




ARKOON Manager 3.0 : 192.168.11.251 (configuration courante)
Fichier Objets Actions Affichage ?
Objets réseaux
arkoon1
Interfaces
Routes statiques
Accès Internet
DNS
NTP
Authentification
Relais
Module VPN
Serveurs VPN autorisés
Interfaces d'écoute
Alertes et journaux
Surveillance système
Reporting (inactif)
IDPS
Autorité de certification (CA
Hôtes
Réseaux
Groupes
Serveurs d'authentification
Services
Catégories
Horaires
Utilisateurs
Certificats
Objets VPN
Politique ICMP
Flux
Bande passante
IDPS
Nom
Description
Cible
Internet
Internet
\Objets réseaux\Réseaux\Internet
Serveurs VPN autorisés
Stations et réseaux autorisés à négocier un VPN
Aucune information disponible pour cet objet.


ARKOON Manager 3.0 : 192.168.11.251 (configuration courante)
Fichier Objets Actions Affichage ?
Objets réseaux
arkoon1
Interfaces
Routes statiques
Accès Internet
DNS
NTP
Authentification
Relais
Module VPN
Serveurs VPN autorisés
Interfaces d'écoute
Alertes et journaux
Surveillance système
Reporting (inactif)
IDPS
Autorité de certification (CA
Hôtes
Réseaux
Groupes
Serveurs d'authentification
Services
Catégories
Horaires
Utilisateurs
Certificats
Objets VPN
Politique ICMP
Flux
Bande passante
IDPS
Nom
Description
Cible
adsl0
Interface ADSL C:\Objets réseaux\arkoon1\Interfaces\adsl0
Interfaces d'écoute
Liste des interfaces écoutées
Aucune information disponible pour cet objet.

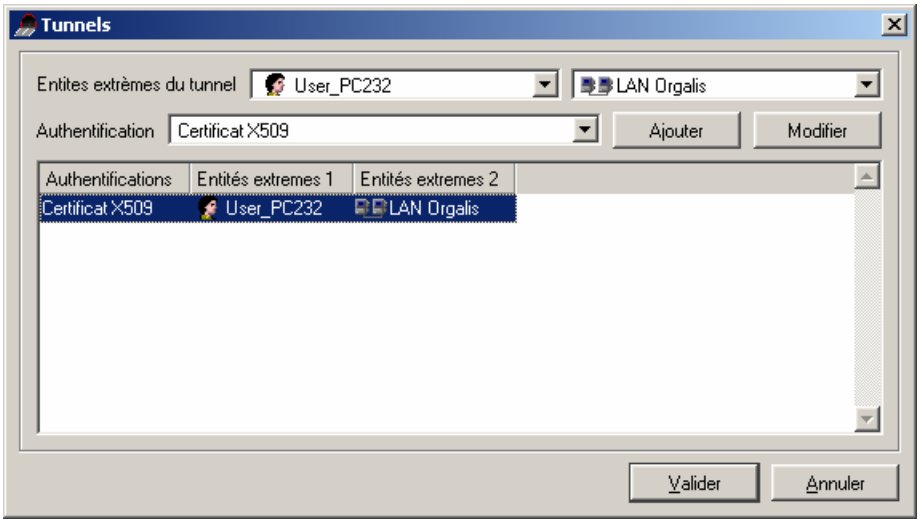
2.4 Paramétrage du VPN



L'objet « LAN Orgalis » doit avoir une passerelle VPN :

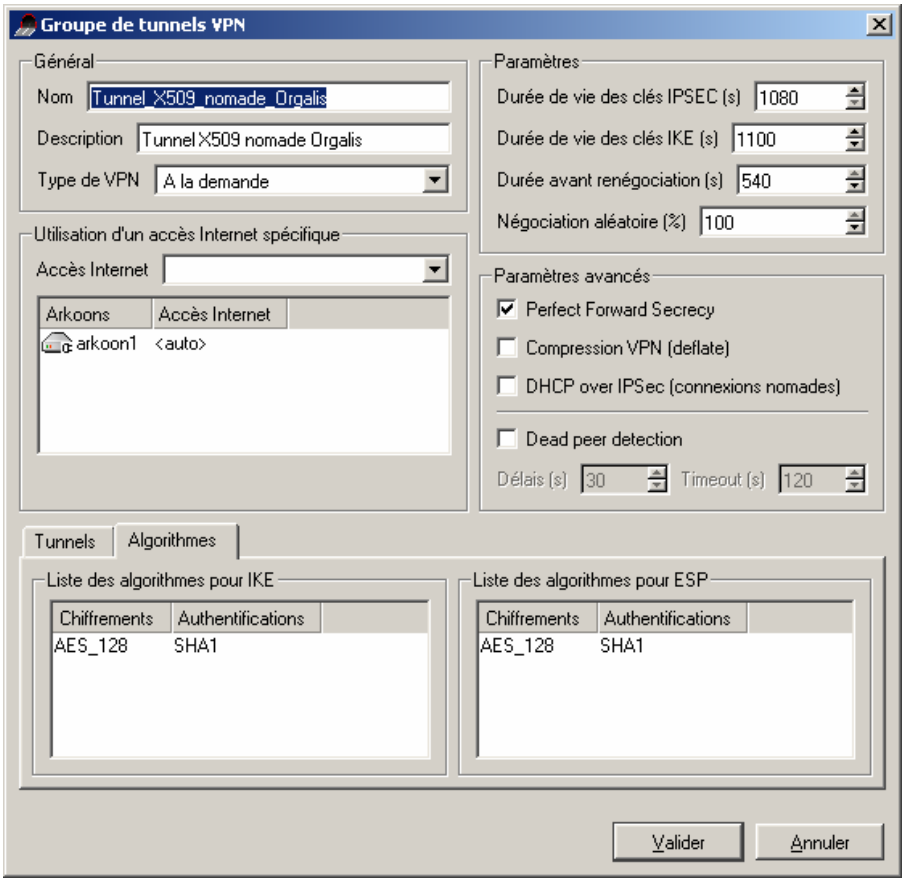
2.5 Définition des entités extrêmes du tunnel VPN

D'un coté un Client VPN IPSec (avec certificat) et de l'autre un réseau local (ou 1 seul hôte, selon le besoin).



2.6 Définition des algorithmes IKE et ESP

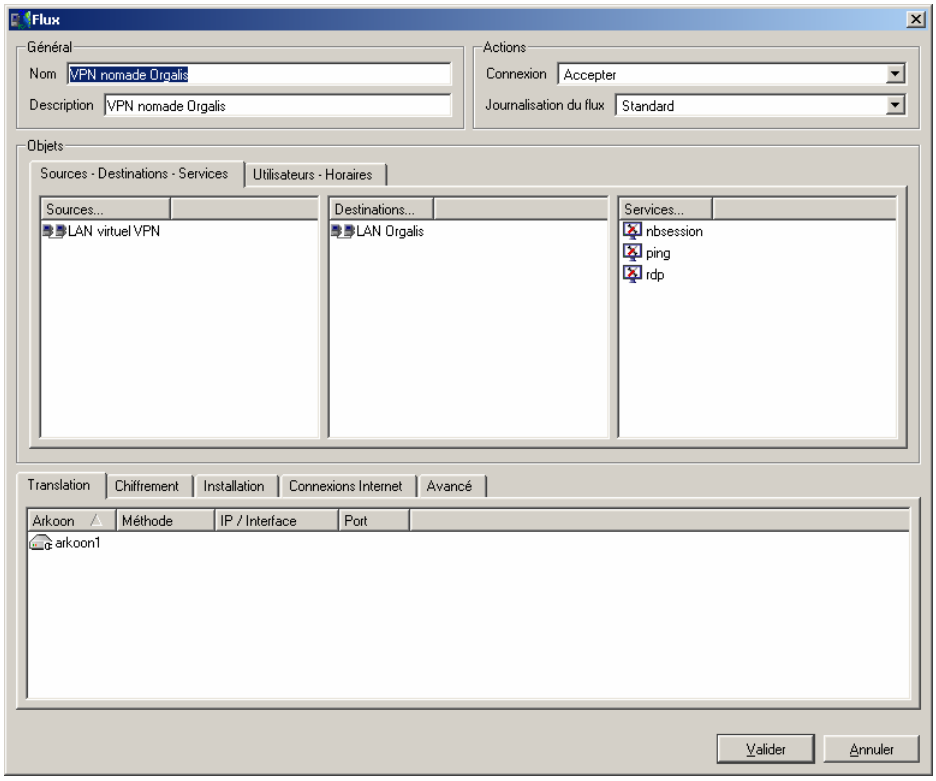
Si aucun algorithme n'est spécifié ici, l'Arkoon s'adaptera à ce que le Client VPN IPSec présentera.



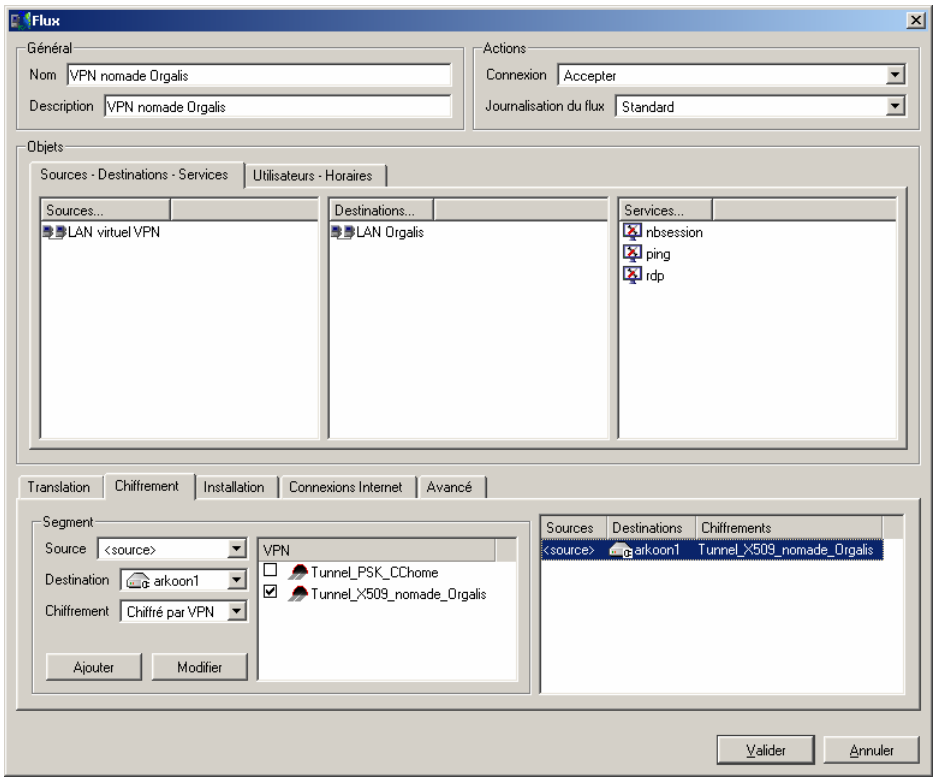
2.7 Création d'une règle de flux

Une règle de flux VPN nomade se positionne en fin des règles, avant bien sur la "default_rule".

Sélectionner la source (LAN virtuel ou Internet), la destination et les services autorisés



2.8 Définition du chiffrement par VPN



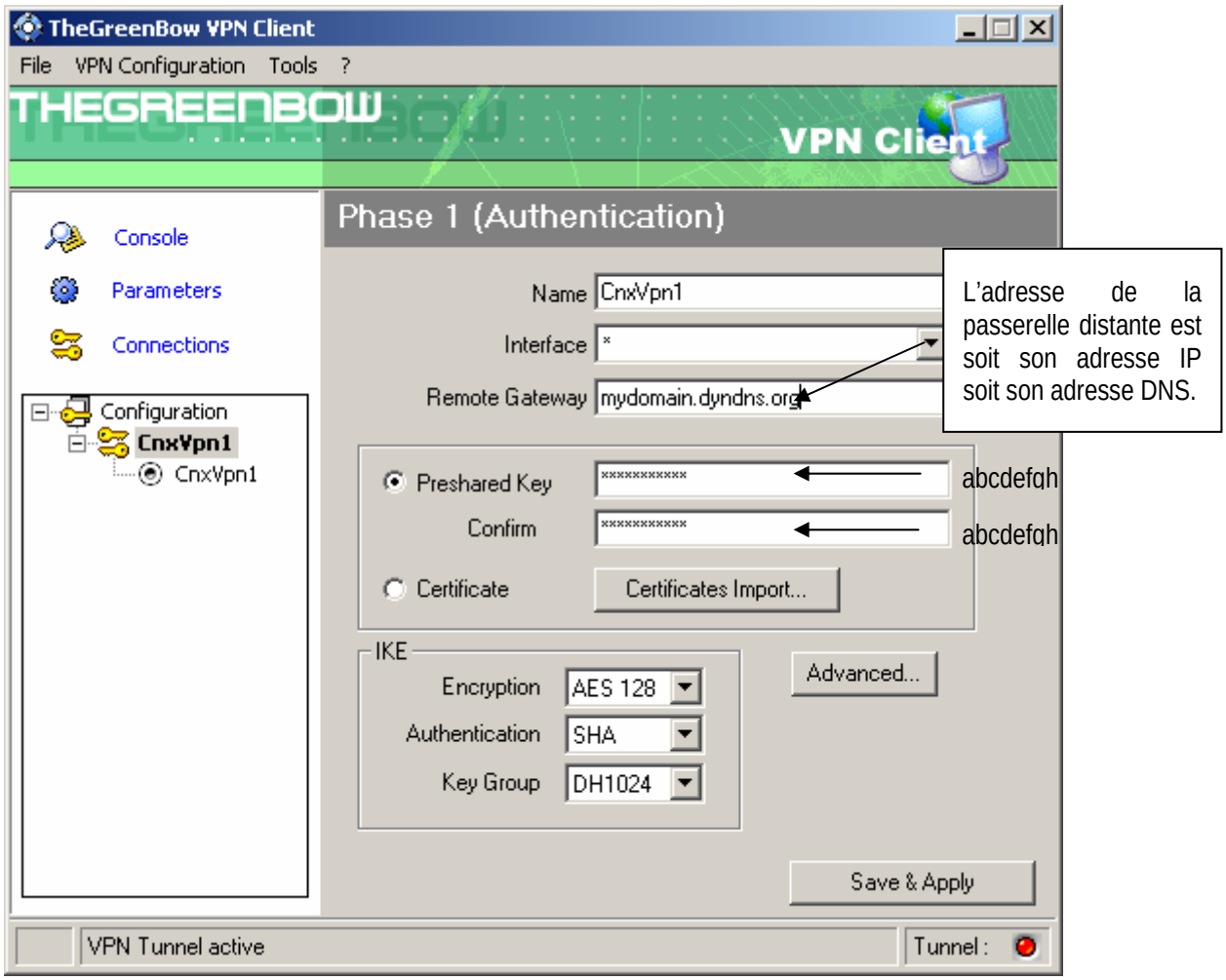
3 TheGreenBow IPSec VPN Client configuration

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.

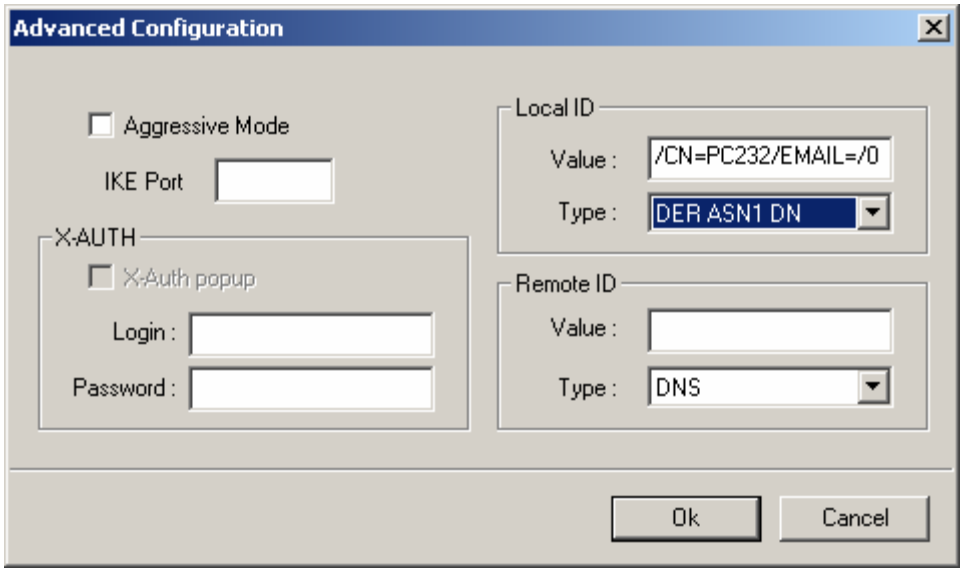
En cliquant sur le bouton "Avancé", vous pouvez configurer Phase 1 IDS et le Mode Agressif.



Configuration Phase 1

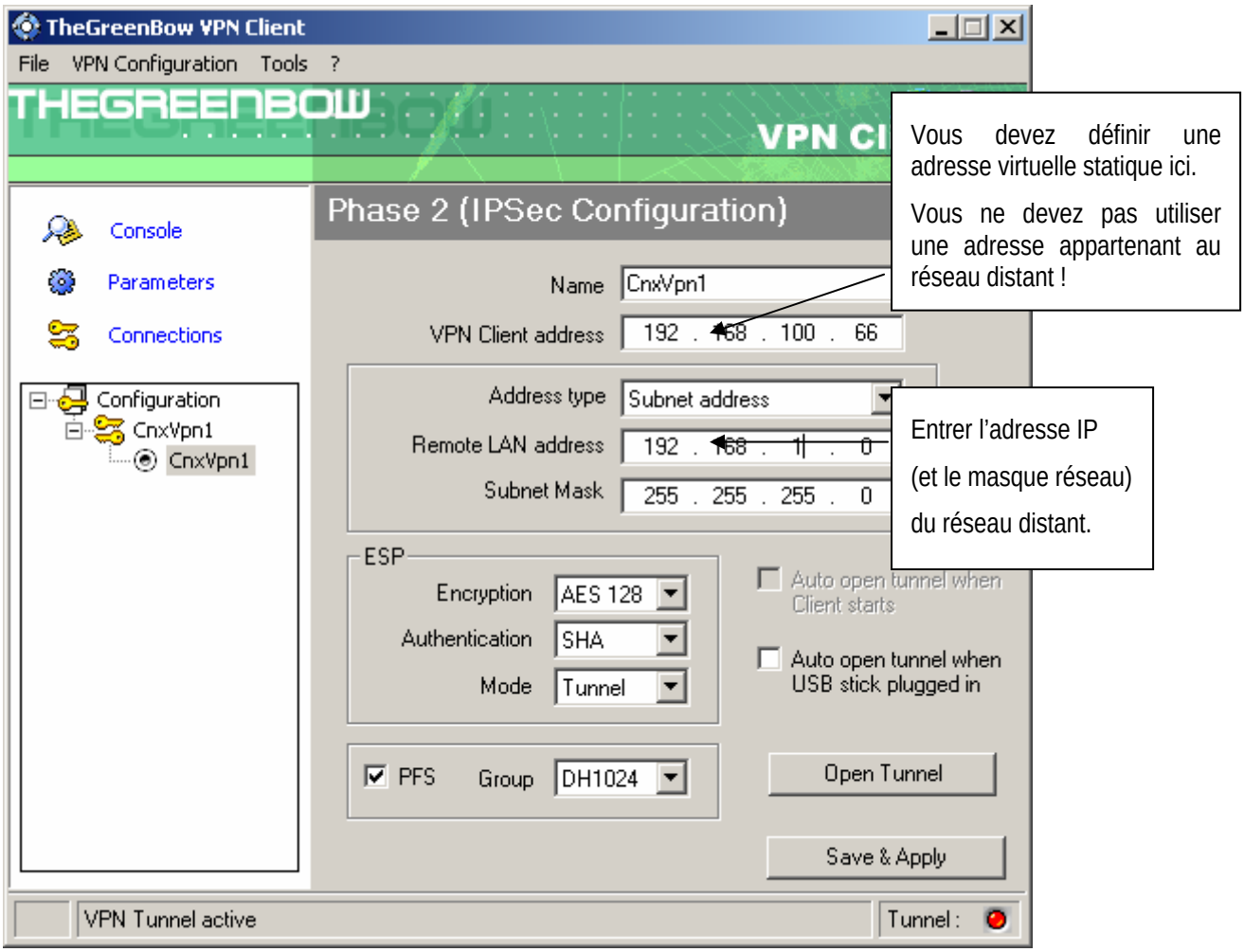
3.2 Certificat Local ID Configuration

Cliquer sur le bouton "Avancé" ou "Advanced" :
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)



3.3 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.

3.4 Ouvrir un tunnel VPN IPSec

Lorsque le Routeur VPN Arkoon 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