Configuration d'un Client Mobile IPSec « TheGreenBow » avec un Firewall Netasq

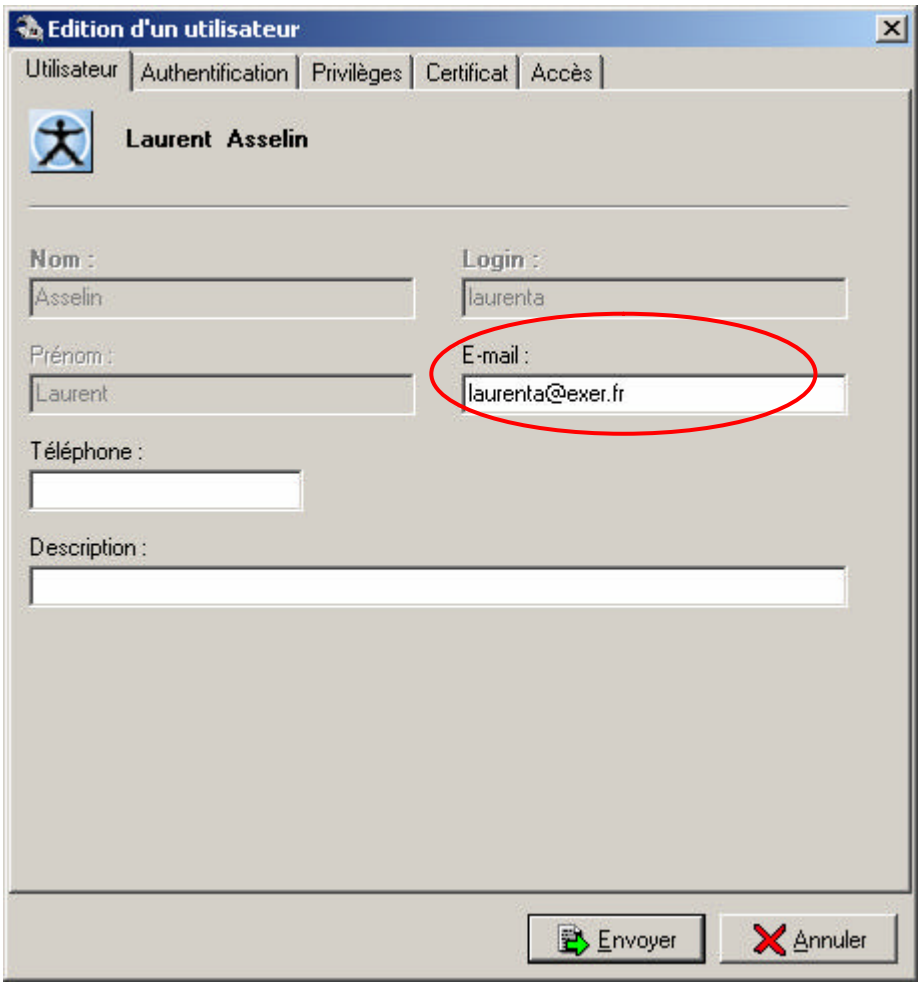
Le but de ce document est de proposer un mode opératoire pour permettre à un utilisateur nomade de se connecter à son réseau d'entreprise via un accès VPN IPSec fournit par un Firewall Netasq.

Nous utiliserons dans les exemples suivants un Firewall Netasq en version 6.2.3 ainsi qu'un client mobile TheGreenBow.

1) Création d'un compte utilisateur dans la base LDAP Netasq

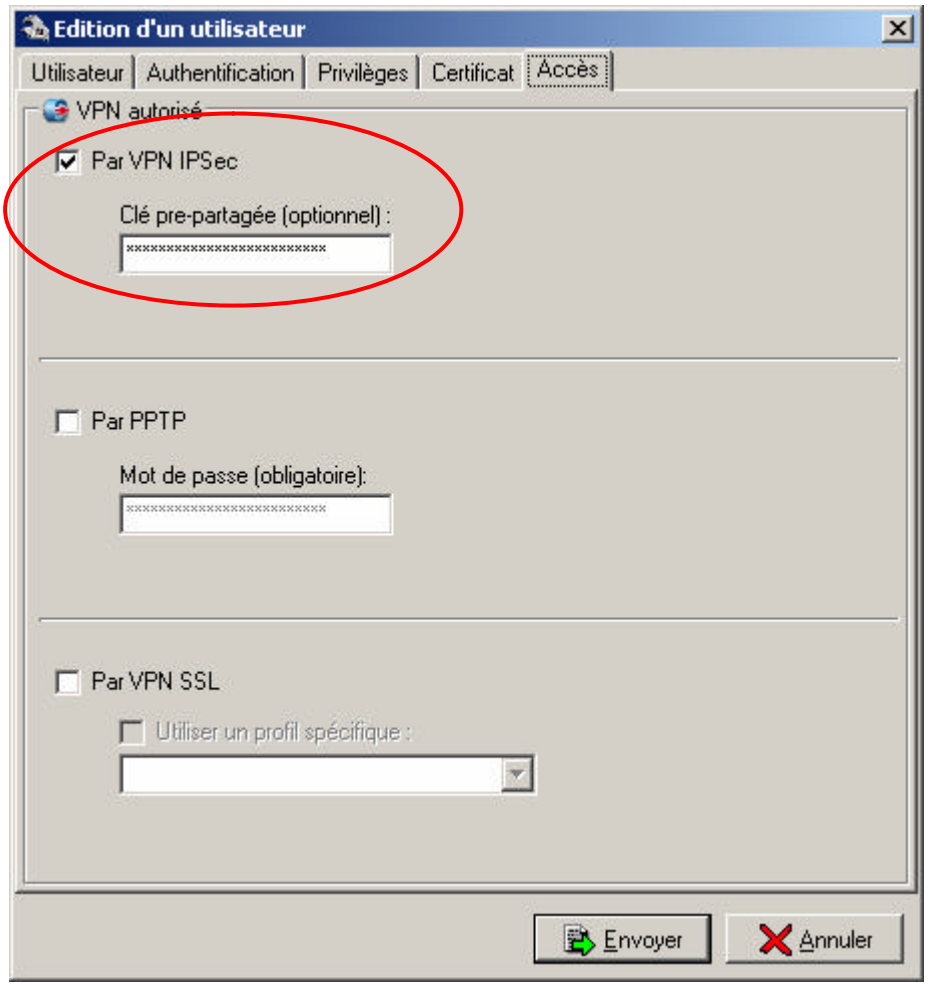
Les utilisateurs nomades se connectant au Firewall depuis des adresses IP dynamiques (HotSpot Wi-Fi, UMTS/Edge, RTC…) , il est impossible de distinguer un utilisateur nomade d'un autre en se basant sur l'IP Source. Pour contourner le problème, Netasq permet l'utilisation de la clef pré partagée pour authentifier de manière transparente un utilisateur.

Nous supposons que la base LDAP Interne du firewall est initialisée. Si vous utilisez une base LDAP Externe, il faut alors modifier son schéma (cf. documentation technique Netasq « na_tn_attributs_001_fr11.pdf »).



Sur cette fiche, il faut impérativement remplir le champ « login » et le champ « e-mail » (c'est l'e-mail qui servira d'authentifiant pour le VPN Nomade).

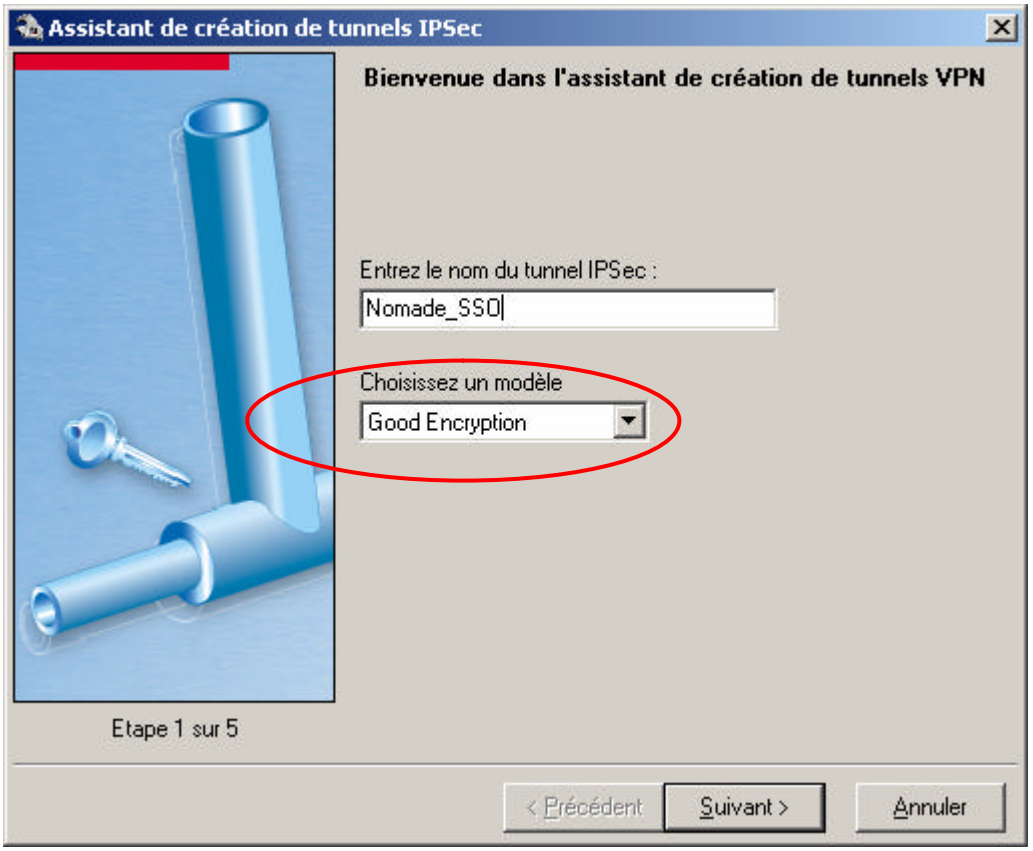
Ensuite, il faut spécifier la clef pré partagée de cet utilisateur dans l'onglet « Accès ».



Il suffit alors d'envoyer pour que cet utilisateur soit créé. Si plusieurs utilisateurs doivent accéder au VPN, il suffit de créer plusieurs objets « utilisateur » en prenant soin d'inscrire un login et un e-mail différents pour chacun.
Pour des raisons de sécurité, il est fortement conseillé que la clé pré partagée IPSec soit différente pour chaque utilisateur).

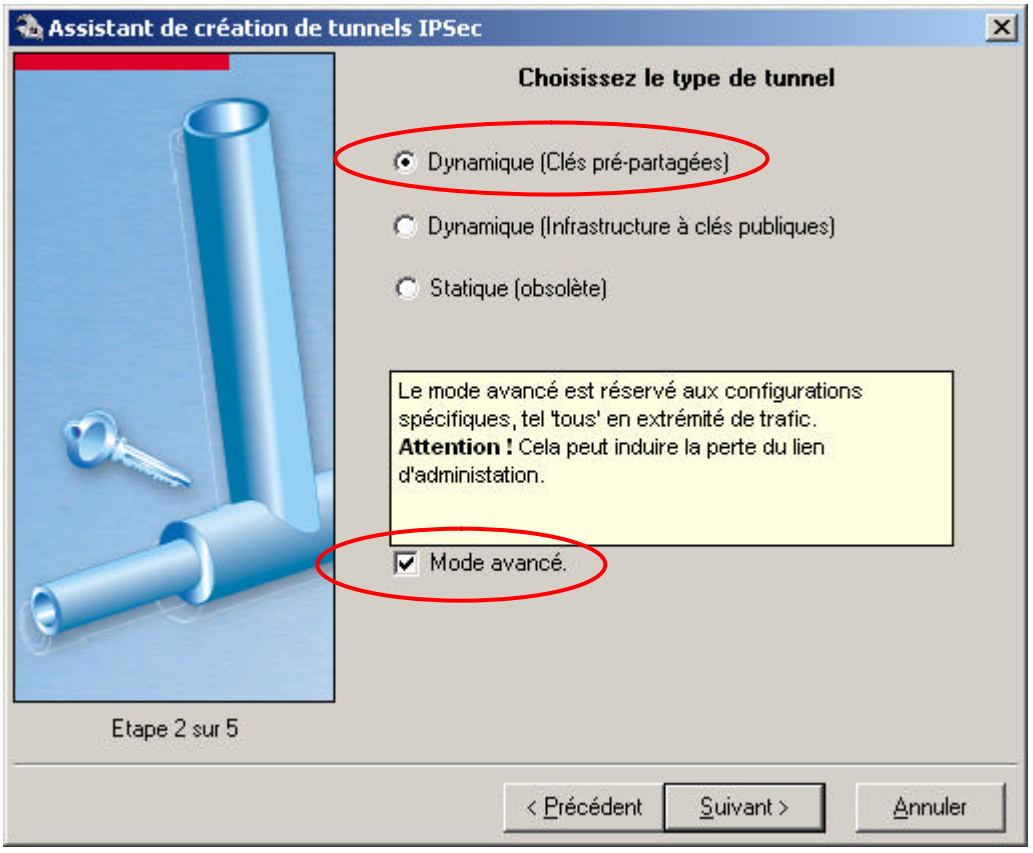
2) Création du Slot VPN sur le Firewall Netasq

Lors de la création d'un nouveau slot VPN, nous sommes aidés par un assistant qui nous demande certaines informations :



Le nom n'a aucune importance, par contre, nous choisissons le modèle « Good Encryption » qui consiste en un pré réglage des algorithmes et des puissances de chiffrement.

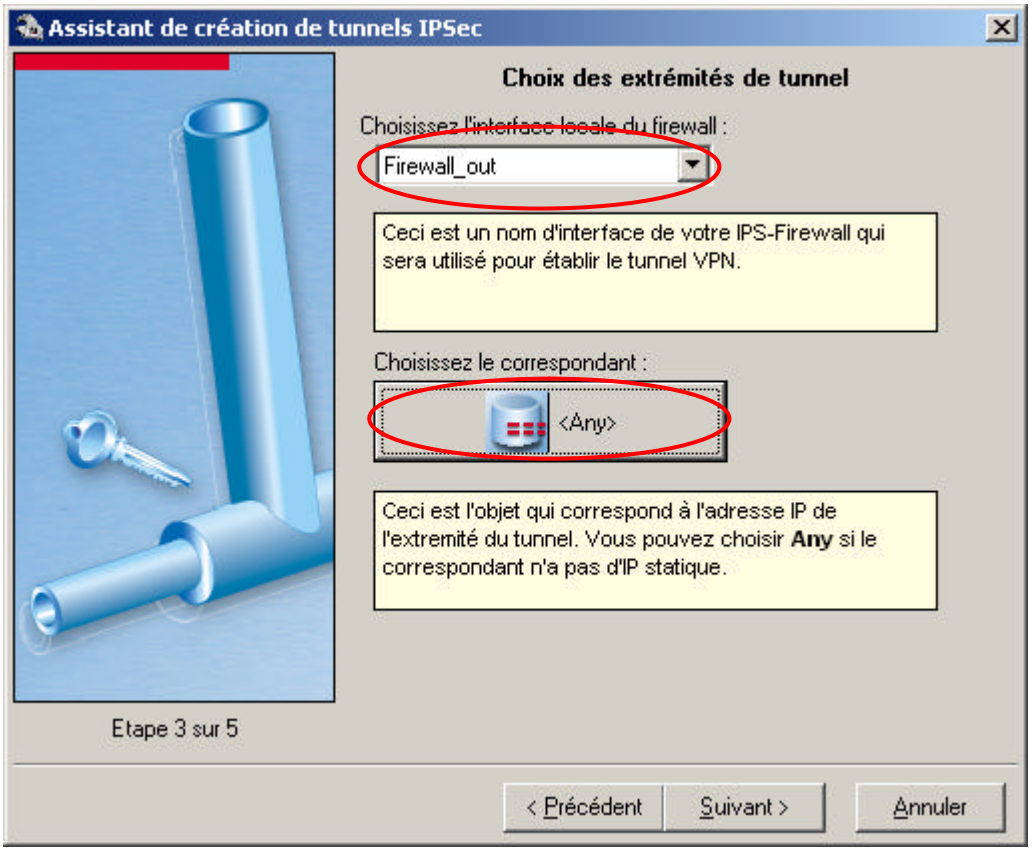
Sur l'écran suivant, nous devons choisir le type de tunnel.
Nous choisissons « Dynamique » et par « Clés pré partagées ».
Ne pas oublié de cocher l'option « Mode Avancé », car nous aurons besoin de définir des extrémités de tunnel et de trafic à « Any » (puisque les nomades se connectent à partir d'IP Dynamiques).



Sur cet écran, nous devons spécifier les extrémités du tunnel VPN.

L'interface locale indique où les flux arrivent, c'est généralement l'interface « Firewall_Out », sauf si l'on utilise une Dialup (PPPoE…) dans ce cas, c'est « Firewall_Dialup ».

Le correspondant indique l'IP Source de l'extrémité distante du tunnel. Dans le cadre d'un tunnel nomade, nous devons choisir « any » (bouton en bas à gauche sur l'interface objets).



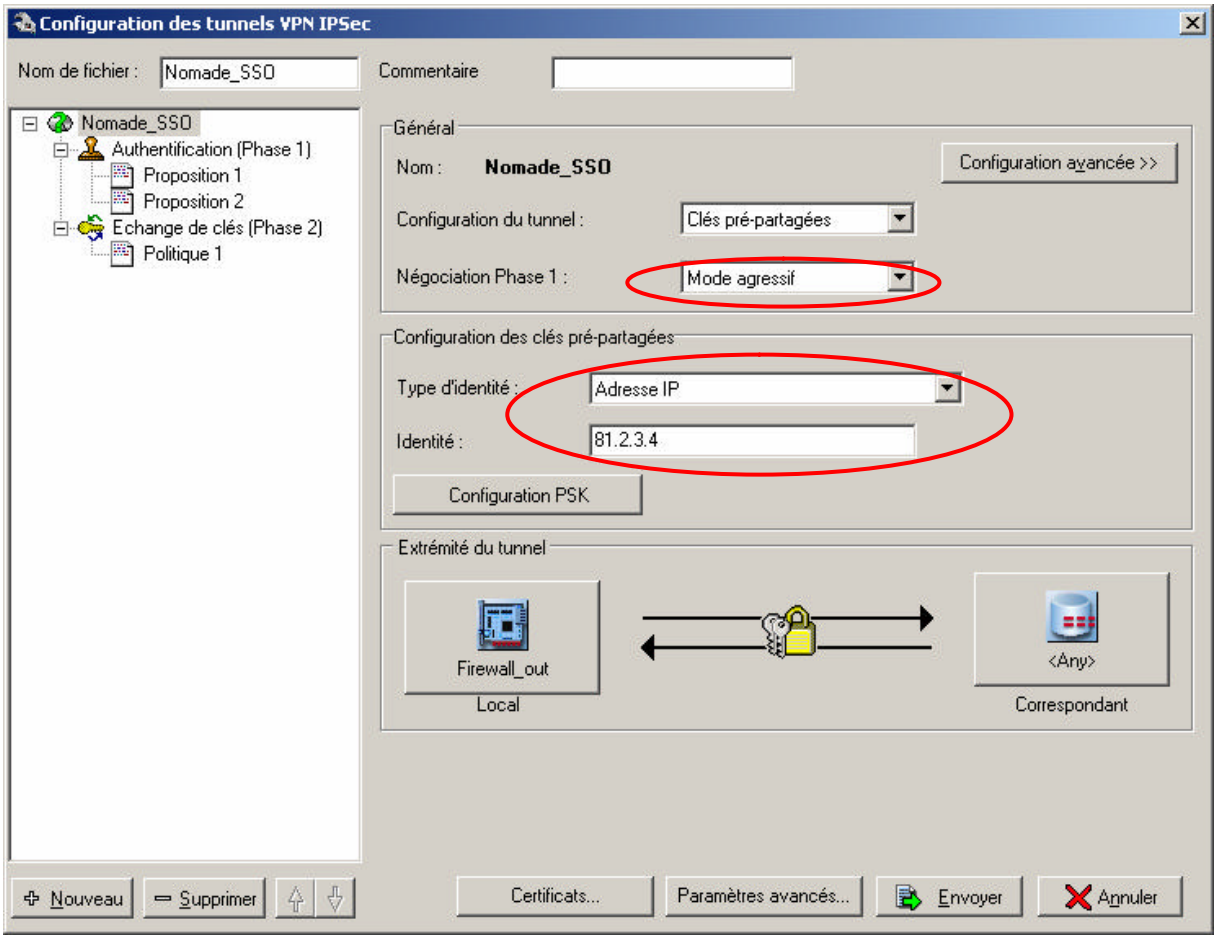
A cette étape, il faut indiquer les extrémités de trafic, c'est-à-dire, entre quelles et quelles machines les données utiles vont communiquées.

La « Machine Locale » correspond au réseau ou à la machine que l'on souhaite rendre joignable par les utilisateurs nomades. C'est un premier niveau de sécurité. Si vous indiquer une machine, vous ne pourrez accéder au maximum qu'à celle-ci, et ce, quelles que soit vos règles de filtrages. Bien souvent lorsque plusieurs machines d'un même réseau doivent être accessibles, on choisit le réseau (exemple « Network_Bridge »), sachant que c'est au niveau des règles de filtrage que l'on précisera quelles machines et quels services seront joignables.

La « Machine Distante » est à nouveau « Any » puisque les nomades se connectent avec des adresses IP changeantes.

Nous arrivons finalement sur la page récapitulative de la configuration du tunnel. Il ne reste plus qu'à modifier quelques paramètres :
La Négociation de Phase 1 doit être changé en « Mode agressif ».
Le Type d'identité doit être mis en «Adresse IP » et il faut entrer l'adresse IP Publique de l'interface du Firewall qui va recevoir les flux VPN.

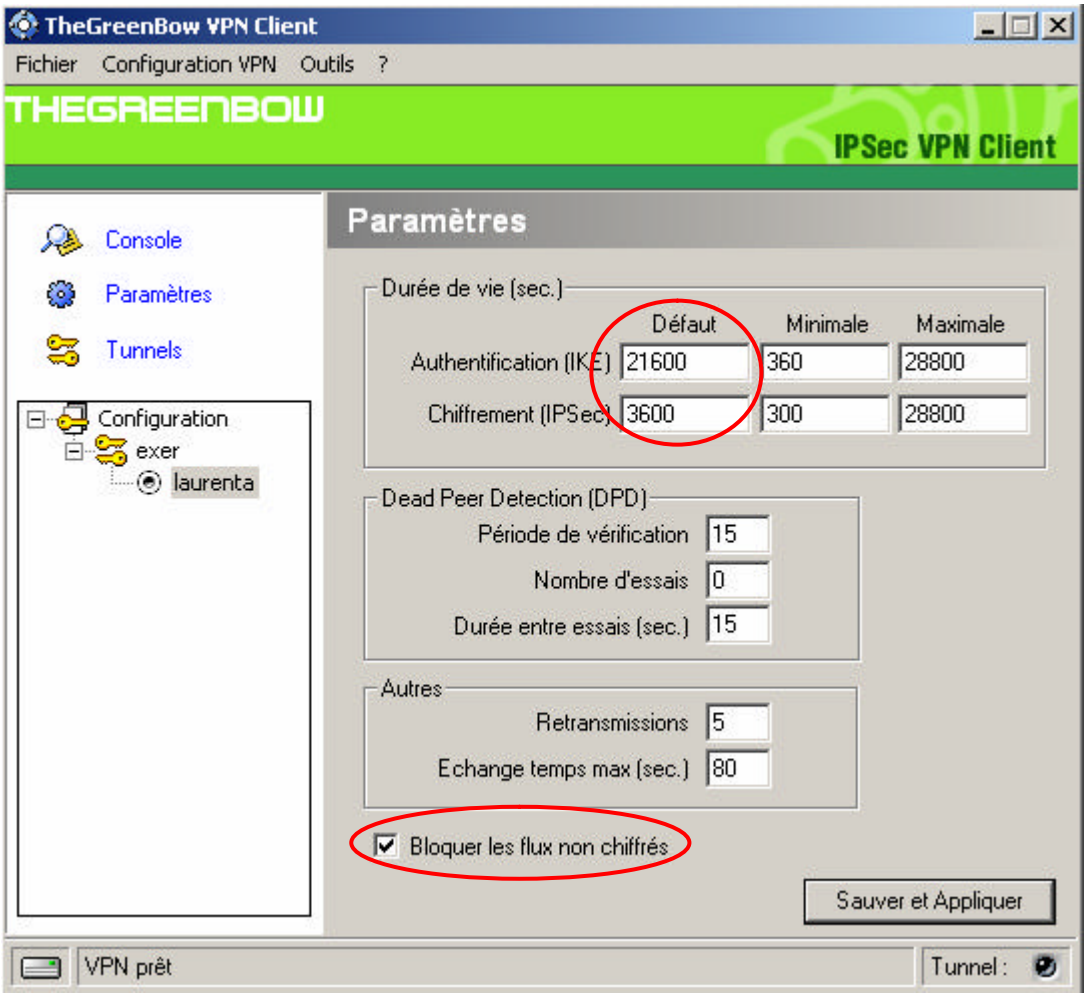
La configuration du VPN au niveau du Netasq est réalisée !



3) Configuration du Client Mobile IPSec TheGreenBow

Sur l'interface du client TheGreenBow il faut créer les deux phases de négociation à savoir la phase 1 correspondant à la négociation IKE et la phase 2 correspondant à la négociation IPSec.

Il faut tout d'abord changer les valeurs par défaut des durée de vie de la session d'Authentification et de Chiffrement dans configuration ? Paramètres et les mettre respectivement à Authentification (IKE) = 21600 et Chiffrement (IPSec)= 3600.

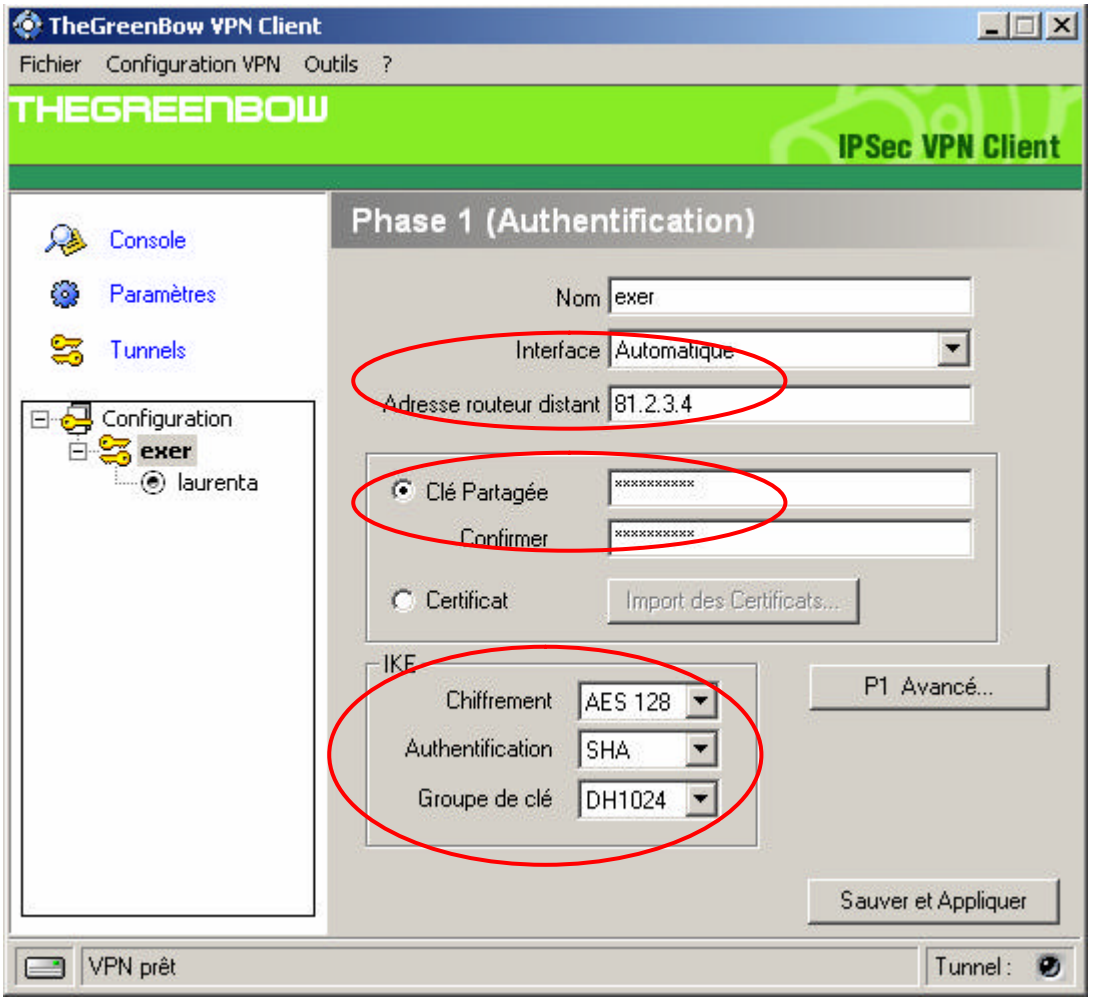


On peut cocher l'option « Bloquer les flux non chiffrés » pour n'autoriser que les flux chiffrés via l'interface du tunnel IPSec.

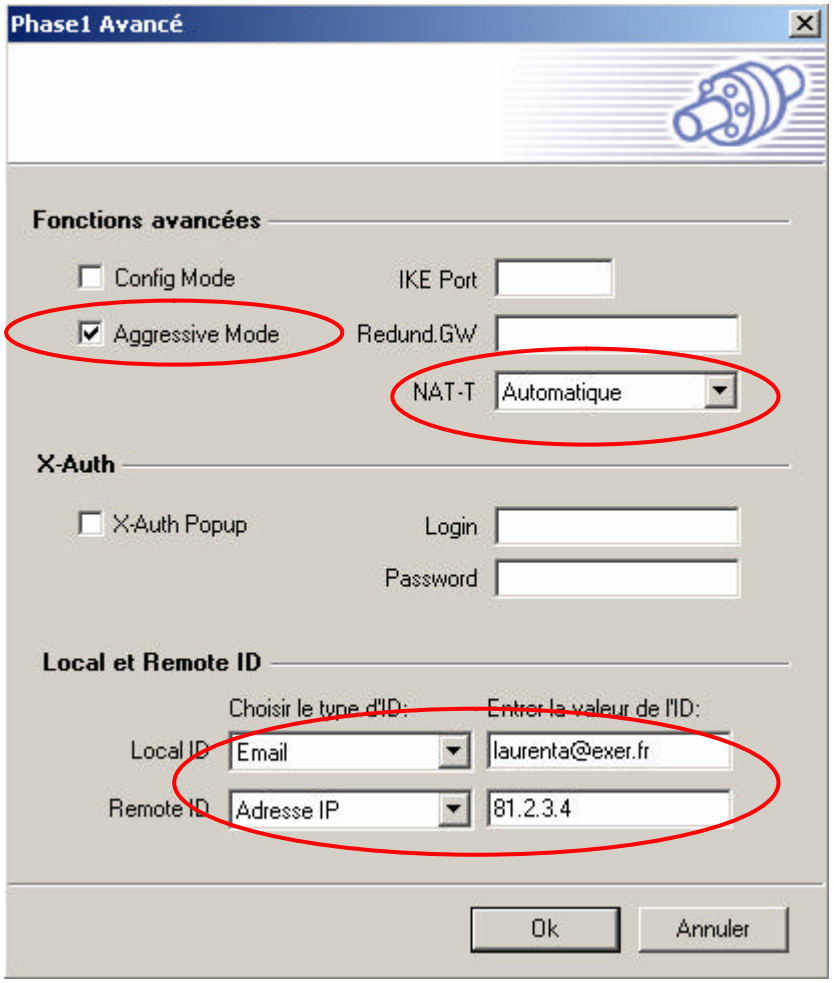
Création de la phase 1

- Durant cette phase, chaque extrémité doit s'identifier et s'authentifier auprès de l'autre. On crée la phase 1 (Configuration VPN ? Nouvelle Phase 1)
  Sur cette première page, on retrouve :
- L'adresse du routeur distant : ceci correspond à l'adresse publique affectée à l'interface externe Firewall_out.
- La clé Partagée avec l'utilisateur que nous crée auparavant dans la base LDAP.
- Les paramètres IKE à savoir Chiffrement : AES 128, Authentification : SHA et le Groupe de clé : DH1024

- Il est important de respecter ces paramètres pour être en accord avec votre configuration VPN du Firewall.



Dans l'onglet P1 Avancé…
- Il faut choisir Aggressive Mode, le NAT-T restant automatique.
- Dans la partie Local et Remote ID, il faut spécifier respectivement l'identifiant que le client VPN envoie au Firewall pour s'authentifier, dans notre cas, c'est une adresse mail préenregistré dans la base LDAP.
- Le Remote ID est l'identifiant que le client s'attend à recevoir du Firewall distant, dans notre cas, c'est l'adresse publique de l'interface Firewall_out.



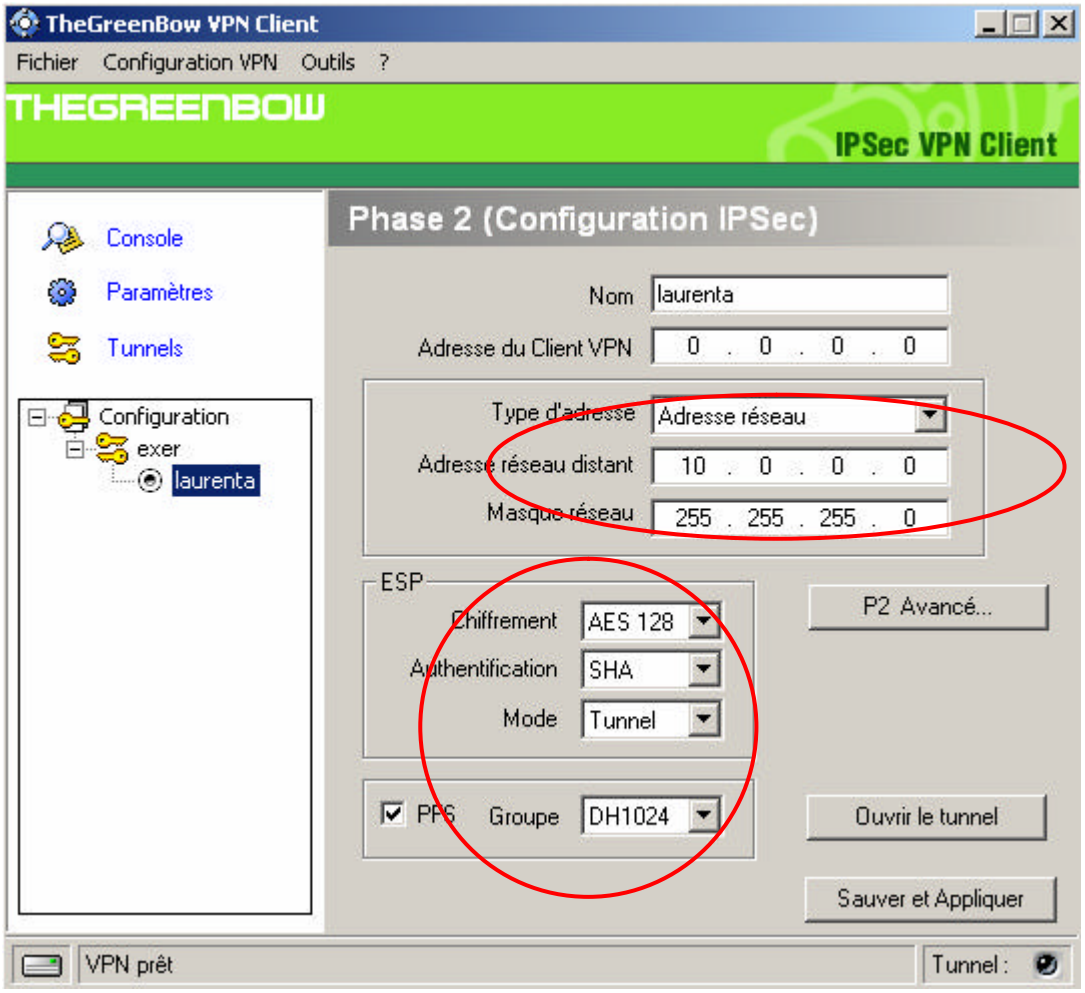
Création de la phase 2

On configure les éléments de la phase 2 dans laquelle on retrouve l'adresse du réseau distant et les éléments du protocole ESP.

Il ne faut rien spécifier dans « Adresse du Client VPN », ce champ doit rester à 0.0.0.0 car lors de la configuration du Firewall, nous avons indiqué au tunnel que le correspondant est Any, il ne peut pas par conséquent avoir une IP fixe en correspondant.

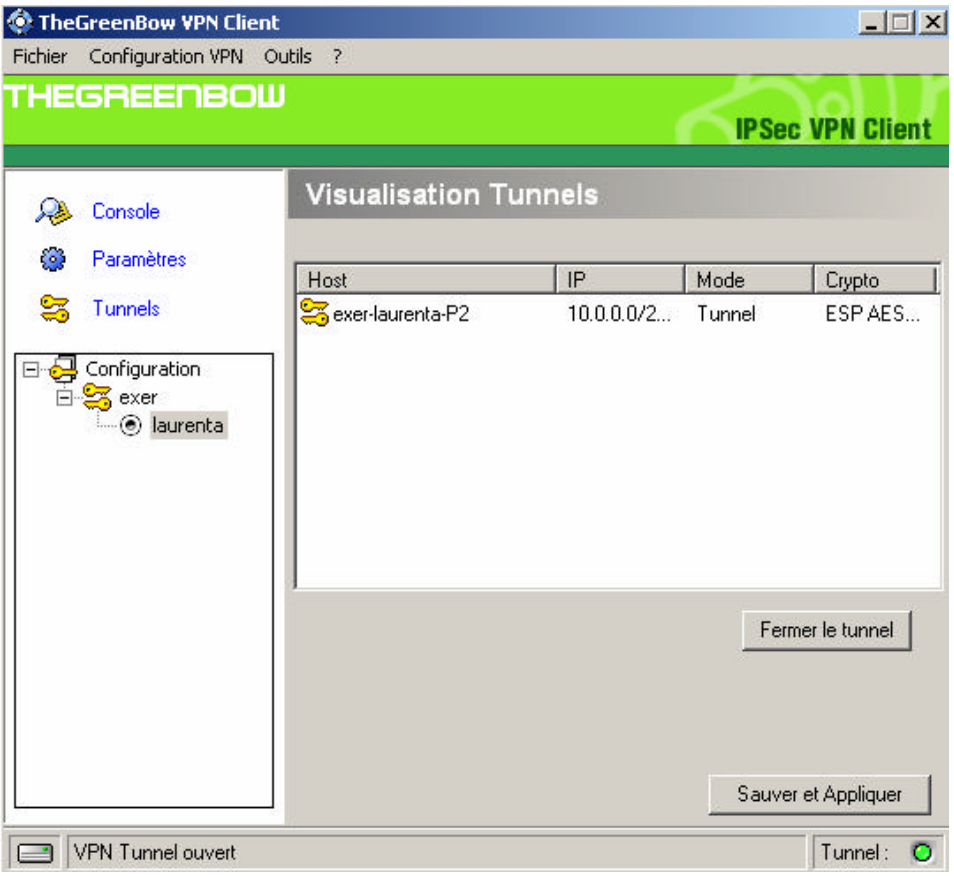
Le réseau distant :
Vous allez renseigner l'adresse de votre réseau local qui sera connecté au tunnel. Il est conseillé de choisir une adresse réseau et d'effectuer les règles de filtrage par la suite.

La partie ESP est toujours AES 128 pour le chiffrement, SHA pour l'authentification et le mode Tunnel.

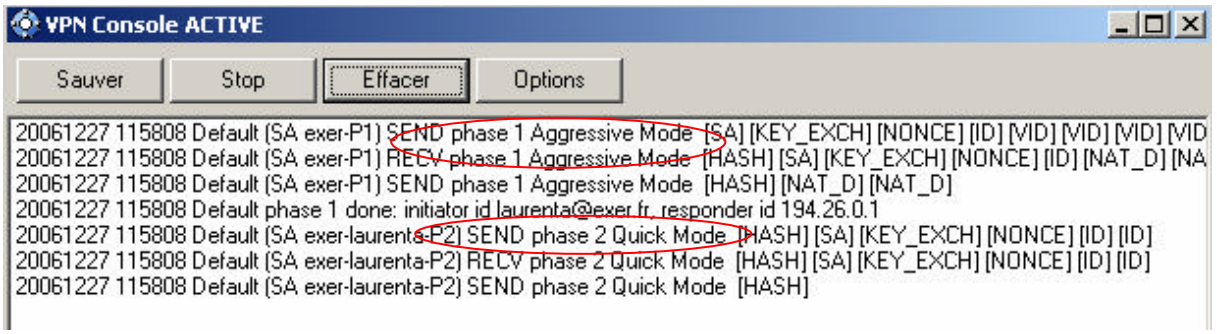


Il ne faut pas oublier de sauver la configuration avant d'ouvrir le Tunnel IPSec et de bien configurer vos règles de Filtrage (essayez en « Pass All » sinon).

Vous pouvez ensuite monter le tunnel en cliquant sur Ouvrir le tunnel et visualiser si vous êtes connecté.

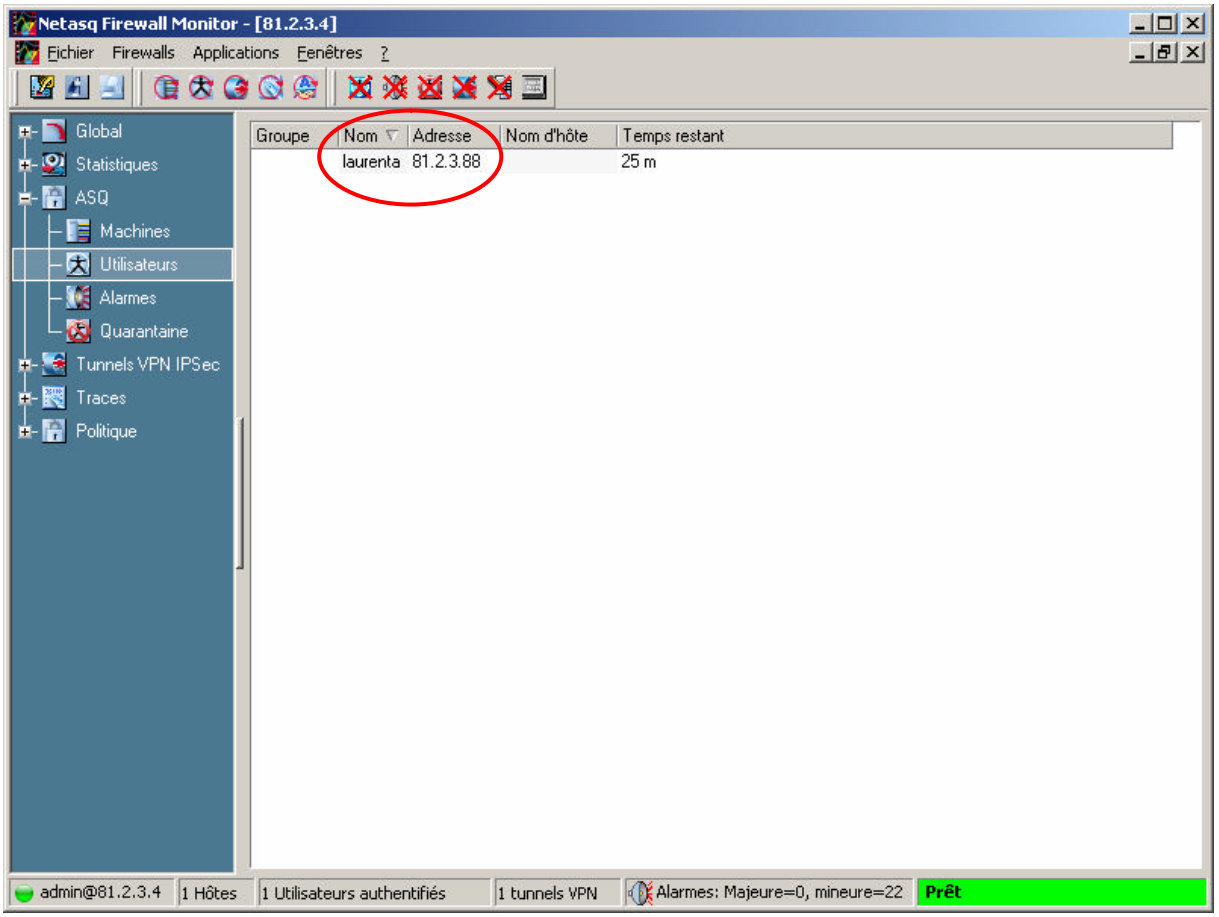


Vous pouvez voir ci-dessous les logs d'une bonne négociation des phases 1 et 2 en allant dans la rubrique console.



4) Vérification de l'authentification auprès du Netasq

Une fois le tunnel établit, on peut vérifier en se connectant sur le Firewall Netasq que l'utilisateur est automatiquement authentifié (grâce à son e-mail).
Ceci va nous permettre de créer des règles de filtrage très strict, puisqu'il nous est possible de distinguer un utilisateur nomade d'un autre.

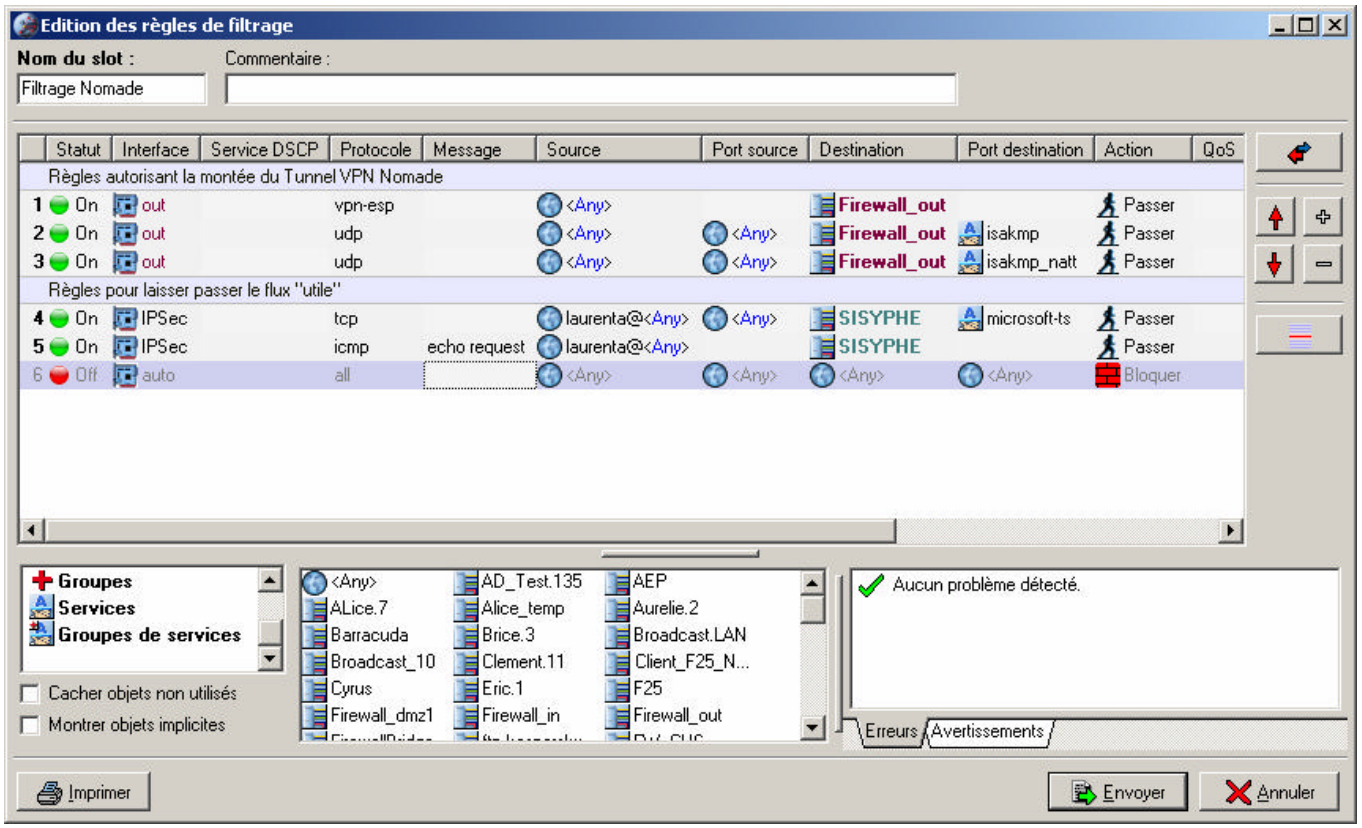


5) Création d'un slot de fitrage

Pour les connexions « nomades », le firewall ne créé pas de règles implicites. Aussi, il faut donc penser à laisser passer les flux en provenance de « Any » et à destination de l'interface publique du Firewall, sur les ports 500/udp, 4500/udp, ainsi que le protocole ESP.

Tout à l'heure, lors de la configuration des extrémités de trafic VPN sur le Firewall, nous avons indiqués en destination le réseau local (Network_In). Toutefois, sans règles de filtrage adéquates, aucun trafic ne sera autorisé à sortir du tunnel.

Voici un exemple de filtrage permettant à l'utilisateur Nomade « laurenta » de se connecter en TSE sur le serveur SISYPHE, via le tunnel IPSec, ainsi que d'envoyer des messages ICMP « Echo Request » (ping) vers ce même serveur.



Notez l'interface source « IPSec » pour spécifier que les flux doivent provenir du tunnel.
Notez également la syntaxe spécifique de la source «laurenta@any » ceci indique que n'importe quelle IP Source est acceptée, à condition que l'utilisateur « laurenta » soit connecté sur le poste.

J'espère que cette documentation vous aura aidée !

Bien Cordialement,

Ahmad SAIF EDDINE