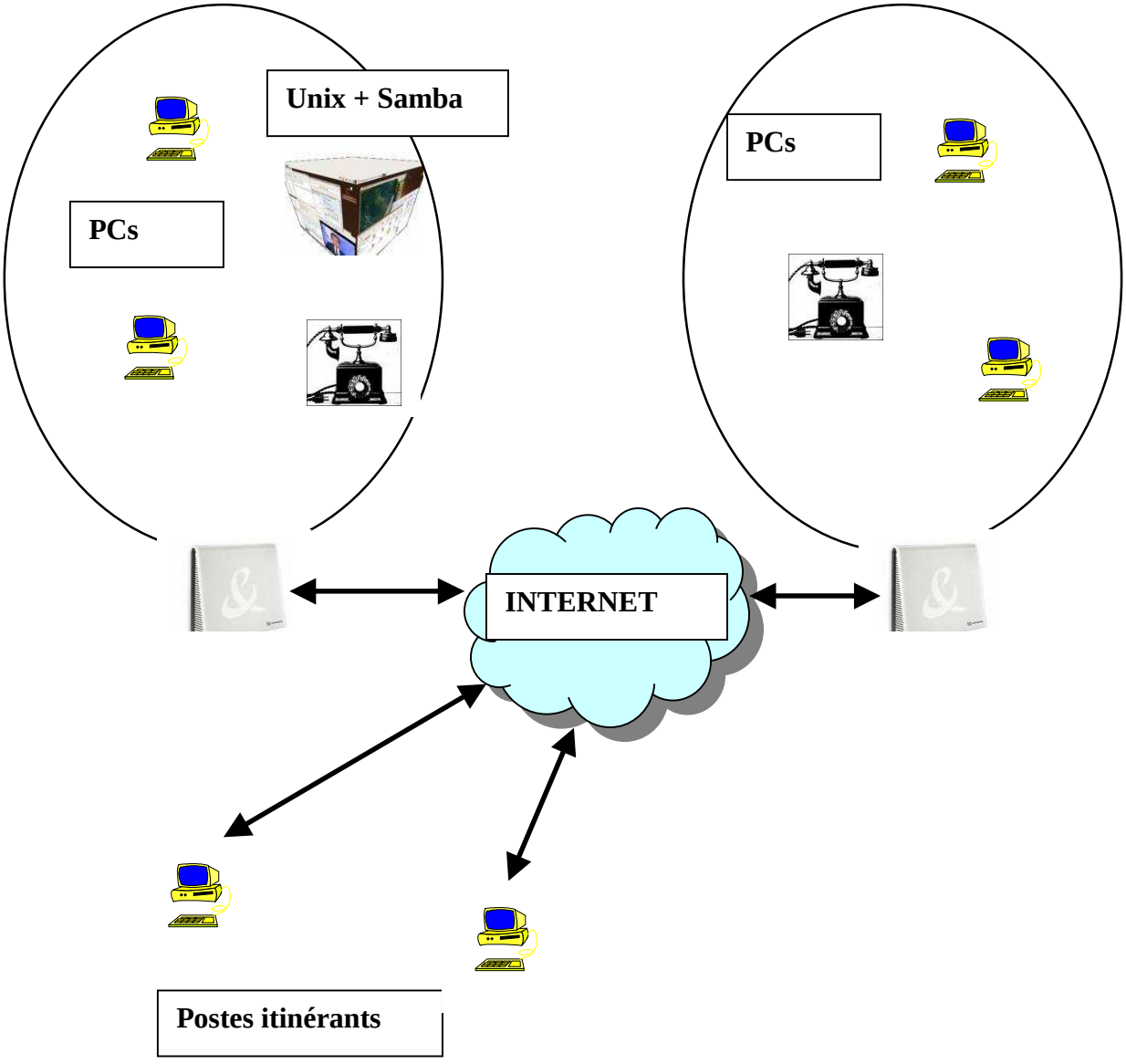
Etablir un tunnel VPN entre deux réseaux.

L'objectif de créer un tunnel VPN entre deux réseaux est de pouvoir faire communiquer n'importe quel système de l'un des réseau avec l'autre, et ce, en toute sécurité.

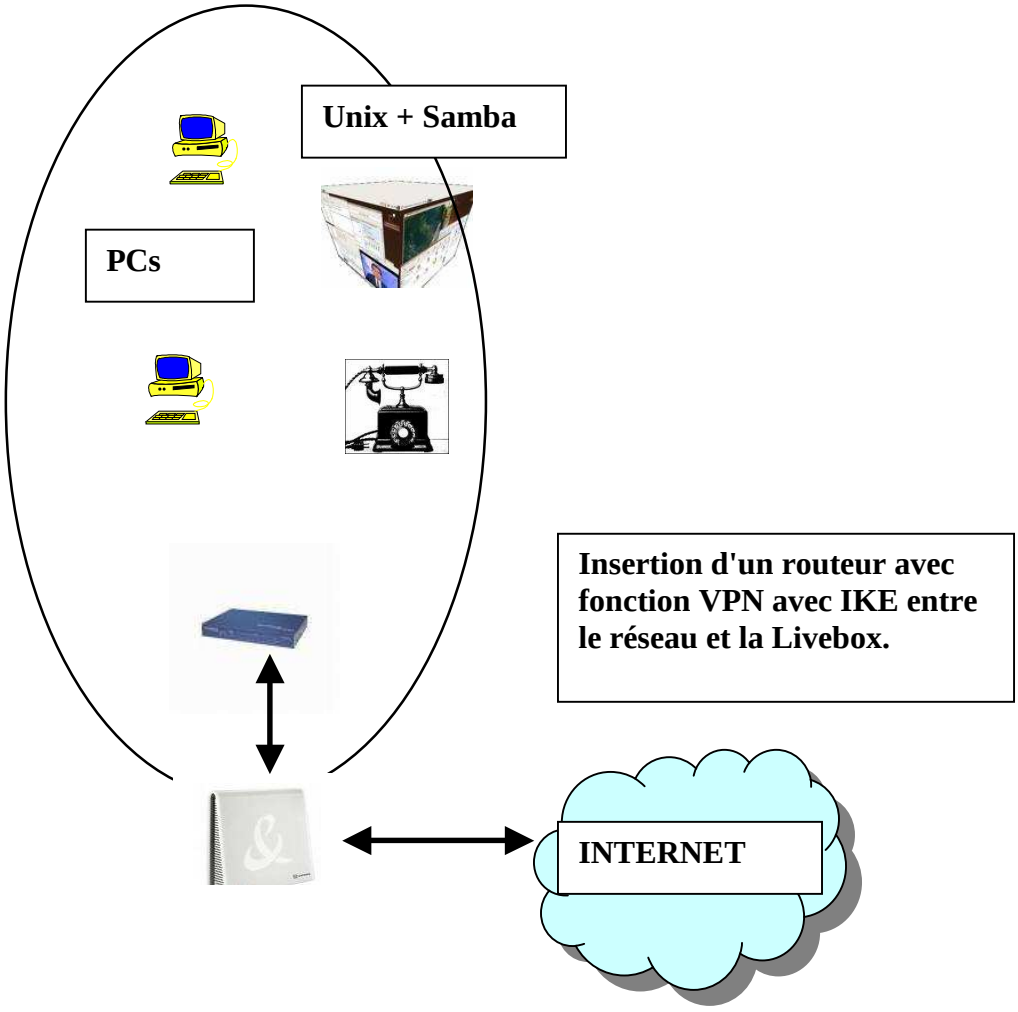
Dans ce tutoriel seront abordés les notions d'authentification et en particulier le protocole IKE.

La configuration des réseaux est la suivante :

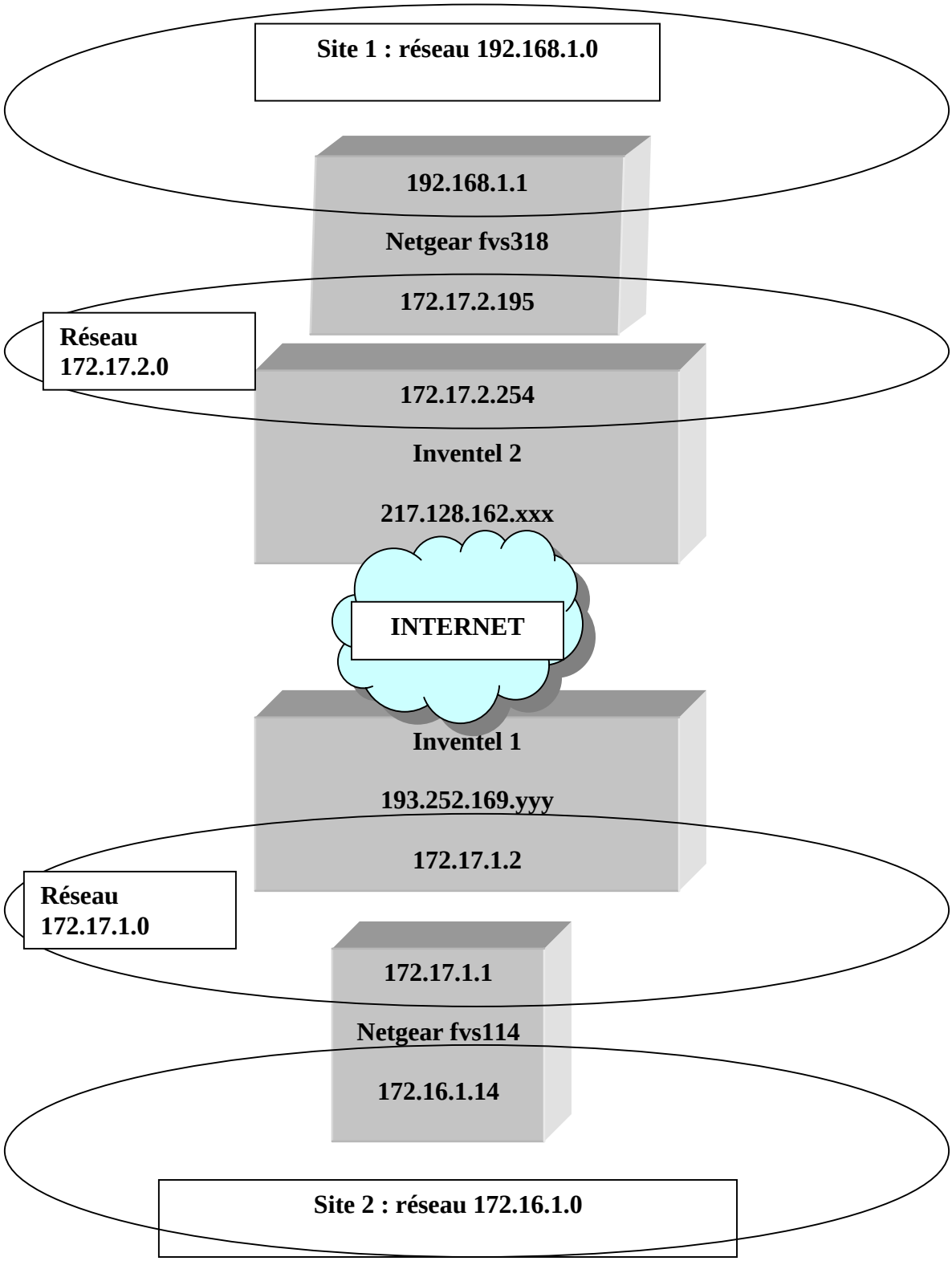


Dans la configuration ci-dessus, les systèmes sont hétérogènes. On doit pouvoir accéder aux imprimantes et aux répertoires partagés, ainsi qu'aux applications de gestion. La "Livebox" ne possède pas de fonction VPN et doit être conservée à cause du téléphone.

La solution adoptée.



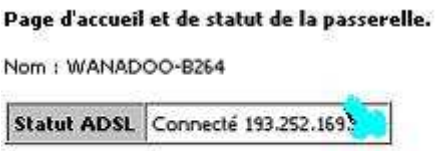
Configuration IP des réseaux.



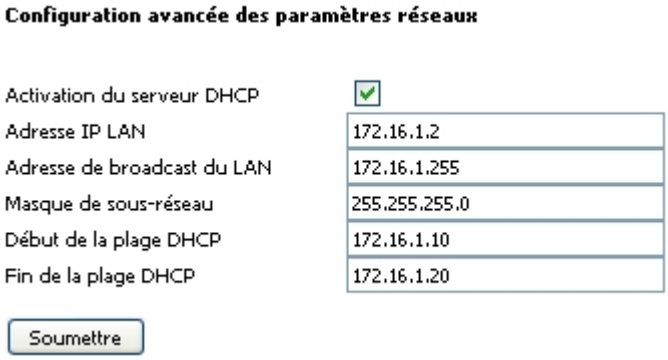
Configuration IP des routeurs.

Connecter une station sur la Livebox et connectez vous avec Firefox à l'adresse IP par défaut (192.168.1.1). Effectuez les modifications qui concernent IP. Il faudra faire ces manipulations de façon symétrique pour chaque réseau.

Ceci est la page d'accueil de la Livebox et l'adresse IP est une adresse IP fixe donné par le FAI.

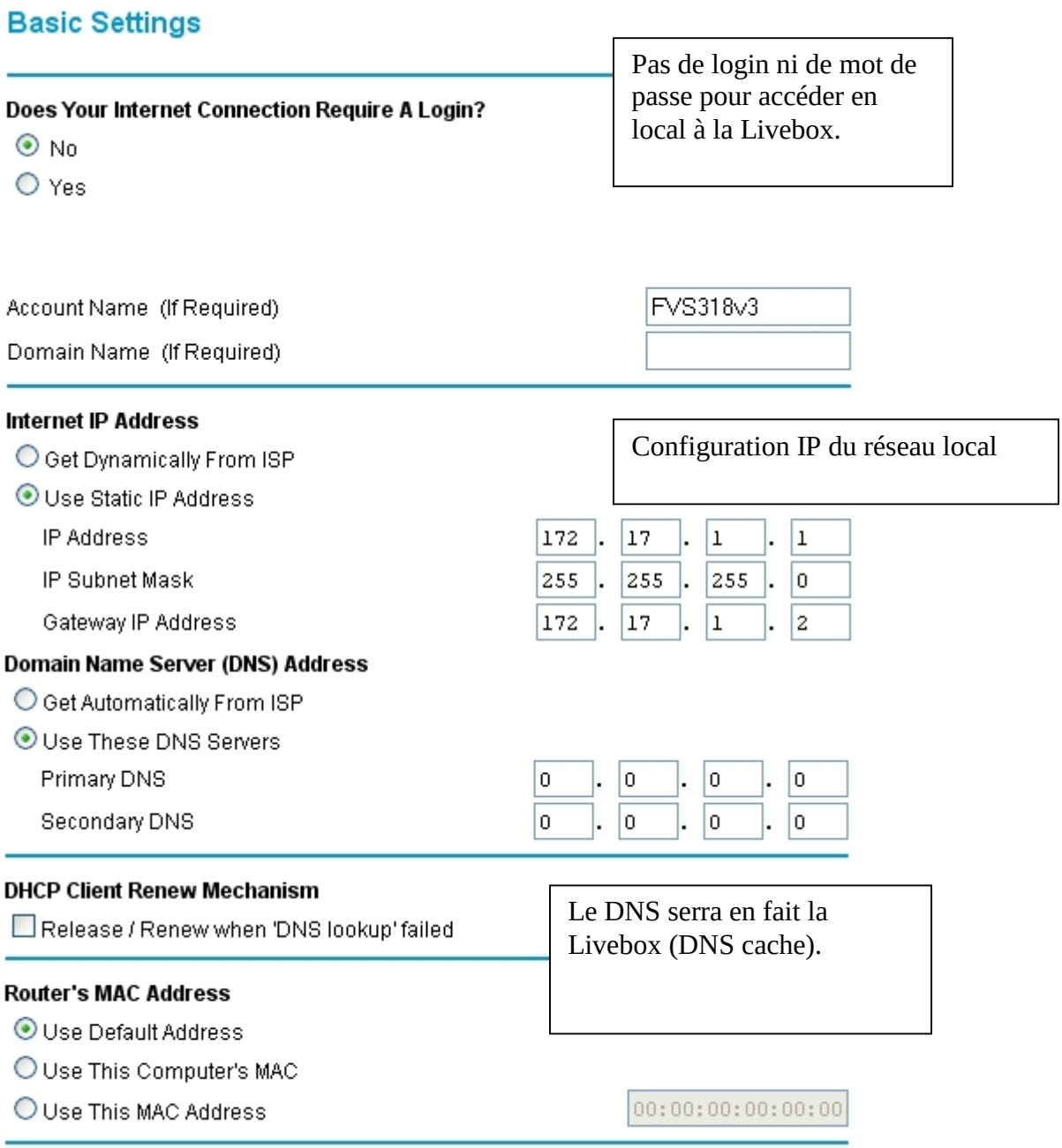


Modifiez l'adresse IP LAN par rapport au réseau local et activez DHCP.



Configuration réseau du routeur (Netgear).

Connectez une station sur le routeur (ici Netgear). Paramétrez la connexion Internet (en fait, vers la Livebox) comme suit.



Connexion des routeurs.

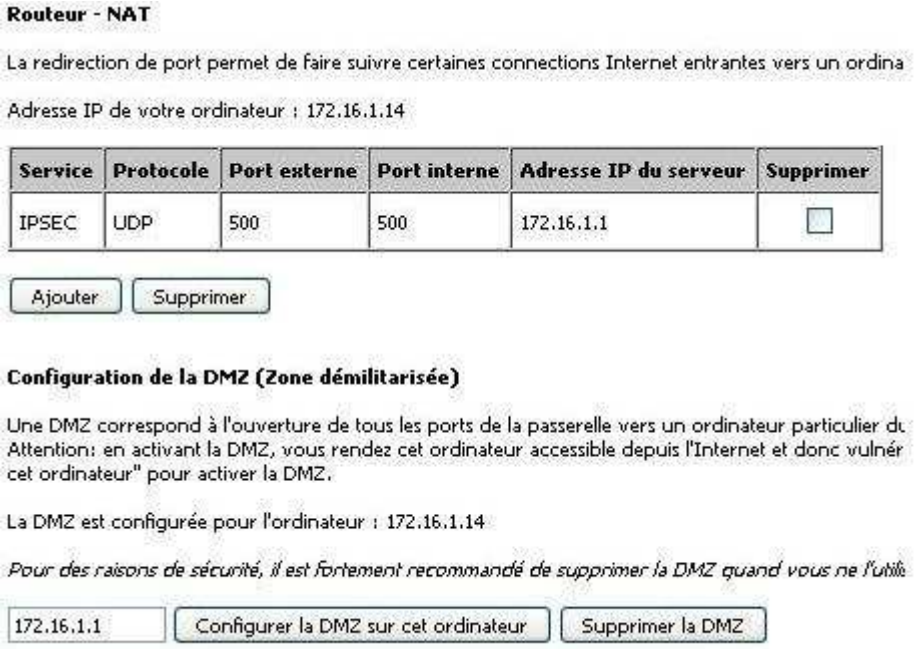
Connectez le port ADSL du routeur Netgear sur un port LAN de la Livebox

Connectez votre station à un port LAN du routeur Netgear.

Testez vos connexions. En faisant un ping à l'adresse IP du premier routeur puis un ping à l'adresse IP de la Livebox et enfin en vous connectant sur Internet.
Si tout fonctionne, alors les connexions et adresses sont bonnes.

Configuration du VPN

Configuration de la Livebox.



Routeur - NAT

La redirection de port permet de faire suivre certaines connections Internet entrantes vers un ordina

Adresse IP de votre ordinateur : 172.16.1.14

Service	Protocole	Port externe	Port interne	Adresse IP du serveur	Supprimer
IPSEC	UDP	500	500	172.16.1.1	☐

Ajouter | Supprimer

Configuration de la DMZ (Zone démilitarisée)

Une DMZ correspond à l'ouverture de tous les ports de la passerelle vers un ordinateur particulier du
Attention: en activant la DMZ, vous rendez cet ordinateur accessible depuis l'Internet et donc vulnér
cet ordinateur" pour activer la DMZ.

La DMZ est configurée pour l'ordinateur : 172.16.1.14

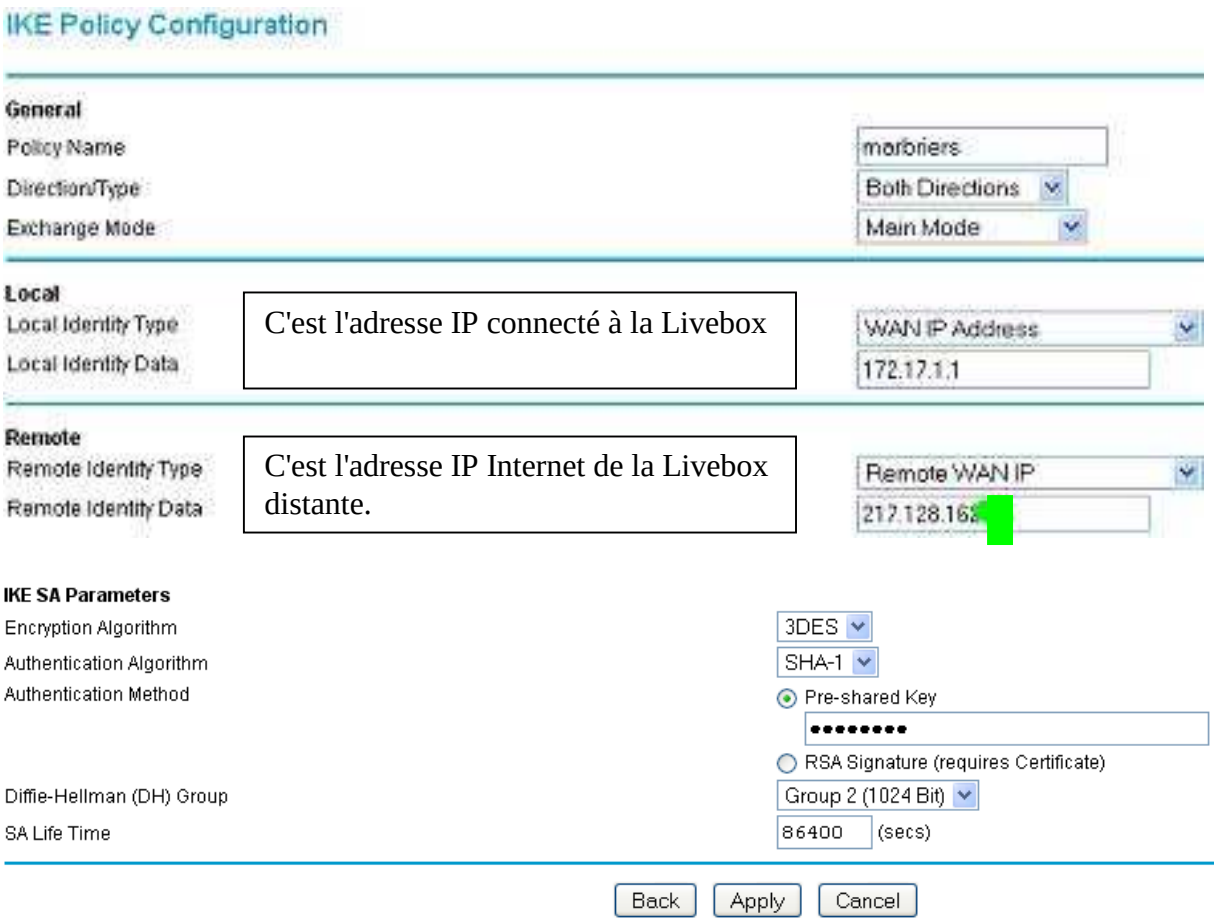
Pour des raisons de sécurité, il est fortement recommandé de supprimer la DMZ quand vous ne l'utili

172.16.1.1 | Configurer la DMZ sur cet ordinateur | Supprimer la DMZ

IL faut rediriger le port 500 qui correspond à IPSEC vers notre routeur Netgear. En outre il faudra mettre le pare-feu de la livebox au minimum.

Configuration du routeur Netgear.

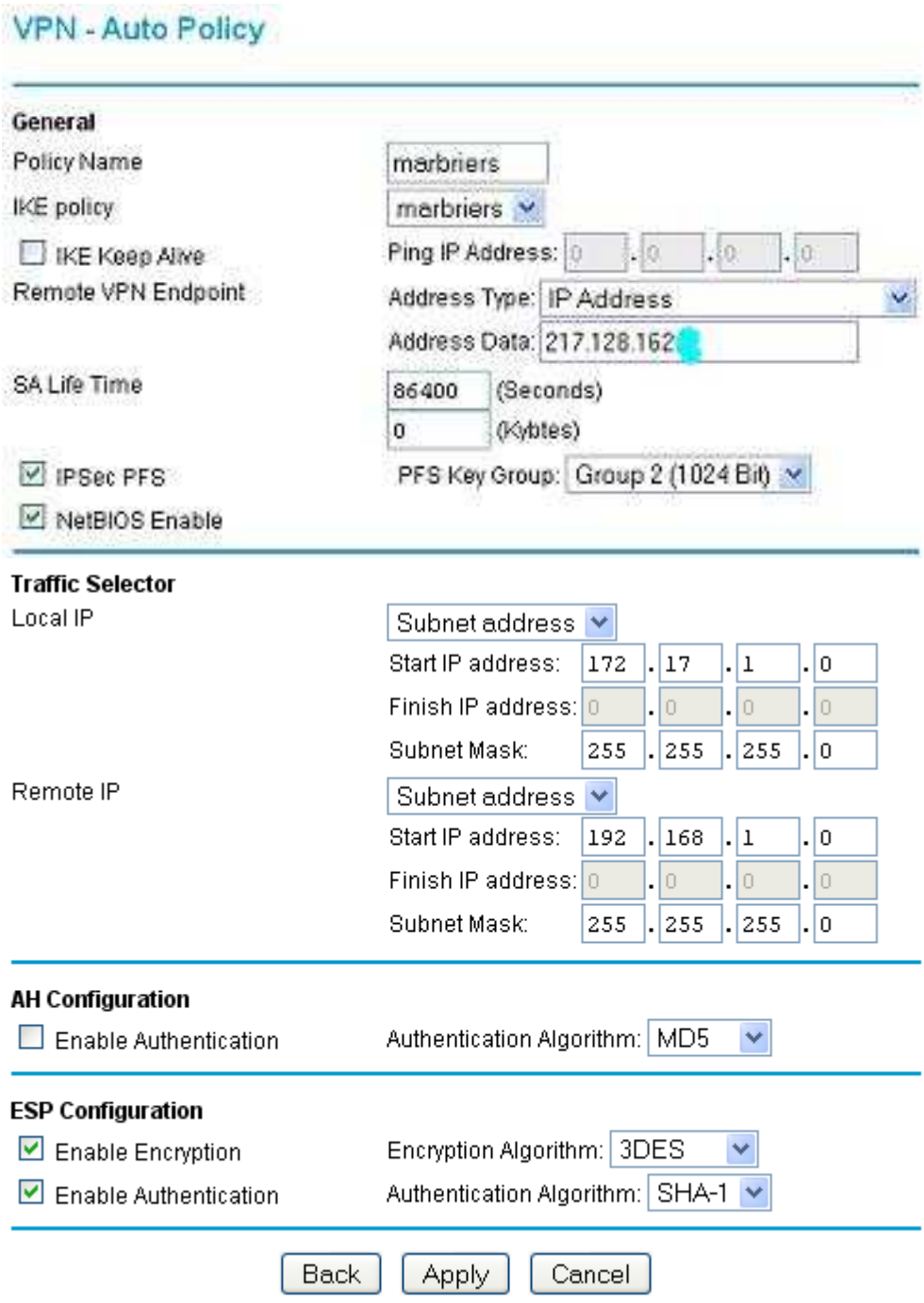
Il faut tout d'abord définir une politique IKE.



Both directions si l'on veut que chaque réseau puisse prendre l'initiative de la connexion.
Main mode est le mode d'identification, l'autre mode est "agressive mode".
Encryption Algorithm est le mode de cryptage 3DES est ici le plus sécurisé.
Authentification Algorithm, ici SHA1 et le plus sécurisé.
La méthode est par clé partagée, la même clé est connue des deux routeurs VPN.

Voir à la fin du tutoriel les informations complémentaires sur IKE.

Configurez la politique VPN



Remote VPN Endpoint : C'est le routeur distant (en fait la Livebox distante).
IPSec PFS : La découverte d'une clé ne permettra pas de déchiffrer tout le message.
ESP Configuration : On définit un algorithme de cryptage et une méthode d'authentification.

Test de la connexion.

Après avoir fait les manipulations sur les deux sites. On peut se connecter avec http sur le routeur Netgear distant.

Cas de Netbios.

La case Netbios Enable a été cochée, mais on ne pourra pas voir les machines de l'autre réseau dans un voisinage réseau via un Explorateur Windows ou un Linneighborhood sous Linux.
En effet netbios découvre les autre machines par trames de diffusion et celles-ci ne traversent pas les routeurs (dans notre cas on a 4 routeurs).
On pourra utiliser les répertoires partagées avec les commandes
sous Windows :

net use x: \\192.168.1.xxx\ressource

ou avec Samba :

smbclient –L 192.168.1.xxx pour voir les ressources et
smbmount //192.168.1.xxx/ressource /point_de_montage

Comprendre IKE.

Pendant le tutoriel un certain nombre de termes et acronymes sont apparus.
IKE SA Parameters, Diffie-Hellman Group, SA life time, IPSec PFS, AH configuration, ESP Authentification, 3DES, SHA-1.

Les modes de cryptage et d'authentification.

Diffie-Hellman.
Méthode de cryptage basé sur le calcul de logarithme discret. Il permet aux deux entités de générer un secret partagé se connaître préalablement.

3DES.
Cryptage par découpage du message en blocs, permutation des blocs, OU exclusif, expension. Ces étapes (rondes) sont répétées 16 fois.

SHA-1.
Méthode de cryptage qui est une fonction de hachage des données. Dans IKE on utilise 3DES pour le cryptage des données et SHA-1 pour le cryptage de l'authentification.

IPSec PFS (Perfect Forward Secrecy).
PFS est un protocole d'échange de clef selon lequel la découverte du secret utilisé ne permet pas de retrouver les clefs de sessions passées et futures.

AH (Authentification Header).
Il assure l'intégrité des données quand on est en mode non connecté (et on est en mode non connecté puisque on utilise le protocole UDP). Un champ est ajouté aux données à protéger, il protège également contre le rejeu par un numéro de séquence.

ESP (Encapsulating Security Payload).
On utilise soit ESP, soit AH. Contrairement à AH ou les données ne sont pas chiffrées, ESP encapsule les données chiffrées et ajoute au debut un numéro de séquence et à la fin des données d'identification.

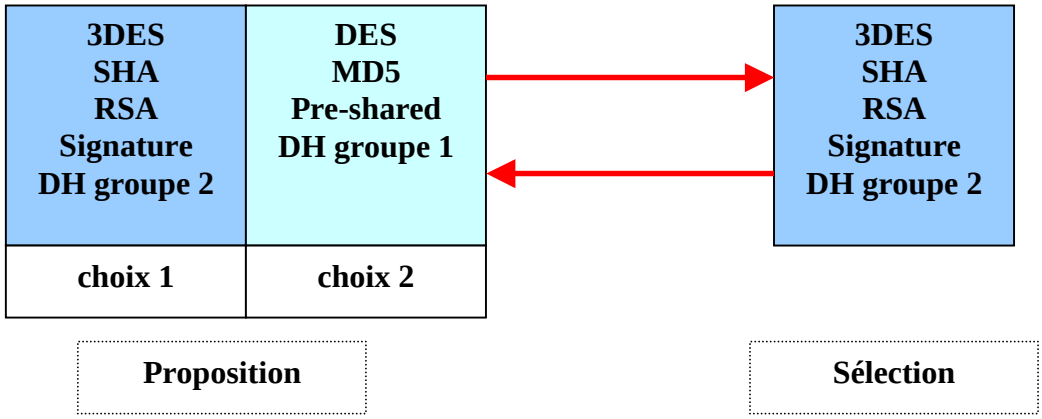
SA Parameters et SA life time.
SA (Security Association) est en fait l'ensemble des paramètres de ESP ou de AH.
Le SA lifetime est donc le temps de vie des paramètres sans renégociation.

Mécanismes IKE.

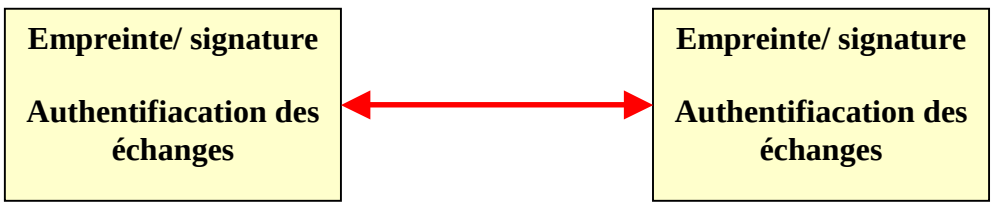
Avant que les messages puissent transiter par le tunnel VPN, IKE va sélectionner le mode de travail et s'assurer de l'identité de l'autre.

IKE agit en deux phases.

Première phase, main mode ou agressive mode : sélection du type de cryptage, de la méthode d'authentification et pour la génération des clés supplémentaires.



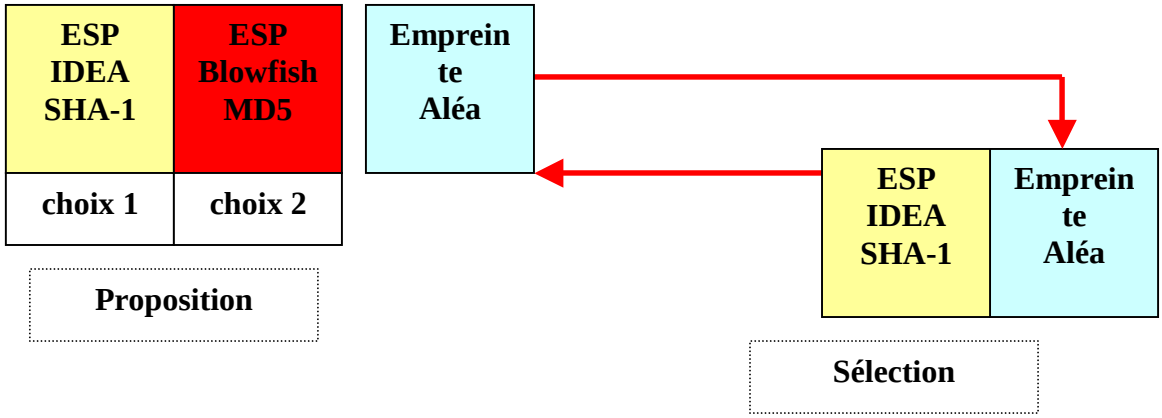
Le secret sert à calculer les clés de session pour protéger la suite des échanges.



Le mode agressif combine les 6 messages ci-dessus pour les ramener à trois. On utilise Agressive mode pour les stations itinérantes qui n'ont pas d'adresse fixe.

Deuxième phase, quick mode :

Cette deuxième phase sert à négocier un ensemble de paramètres de SA, de générer de nouvelles clés et d'identifier le trafic que le SA protègera.



Pour terminer, on pourra voir les phases d'IKE dans les logs de notre routeur.

VPN Status/Log

```
[2006-05-10 07:49:59][==== IKE PHASE 1(to 86.194.16.  ) START (initiator) ====]
[2006-05-10 07:49:59]**** SENT OUT  FIRST MESSAGE OF MAIN MODE ****
[2006-05-10 07:49:59]<POLICY: marbriers> PAYLOADS: SA,PROP,TRANS
[2006-05-10 07:49:59]**** RECEIVED SECOND MESSAGE OF MAIN MODE ****
[2006-05-10 07:49:59]<POLICY: marbriers> PAYLOADS: SA,PROP,TRANS
[2006-05-10 07:49:59]**** SENT OUT  THIRD MESSAGE OF MAIN MODE ****
[2006-05-10 07:49:59]<POLICY: marbriers> PAYLOADS: KE,NONCE
[2006-05-10 07:50:01]**** RECEIVED FOURTH MESSAGE OF MAIN MODE ****
[2006-05-10 07:50:01]<POLICY: marbriers> PAYLOADS: KE,NONCE
[2006-05-10 07:50:01]<ID PAYLOAD> Type = ID_IPV4_ADDR,ID Data=172.16.1.14
[2006-05-10 07:50:01]**** SENT OUT  FIFTH MESSAGE OF MAIN MODE ****
[2006-05-10 07:50:03]**** RECEIVED  SIXTH MESSAGE OF MAIN MODE ****
[2006-05-10 07:50:03]<POLICY: marbriers> PAYLOADS: ID,HASH
[2006-05-10 07:50:03]**** MAIN MODE COMPLETED ****
[2006-05-10 07:50:03][==== IKE PHASE 1 ESTABLISHED====]
```

VPN Status/Log

```
[2006-05-10 07:50:03]**** MAIN MODE COMPLETED ****
[2006-05-10 07:50:03][==== IKE PHASE 1 ESTABLISHED====]
[2006-05-10 07:50:03][==== IKE PHASE 2(to 86.194.16.  ) START (initiator) ====]
[2006-05-10 07:50:03]**** SENT OUT  FIRST MESSAGE OF QUICK MODE ****
[2006-05-10 07:50:03]<Initiator IPADDR=172.17.1.0,PORT=0>
[2006-05-10 07:50:03]<Responder IPADDR=192.168.1.0,PORT=0>
[2006-05-10 07:50:03]**** RECEIVED SECOND MESSAGE OF QUICK MODE ****
[2006-05-10 07:50:03]<POLICY: marbriers> PAYLOADS: HASH,SA,PROP,TRANS,NOTIFY,NON
[2006-05-10 07:50:03]**** SENT OUT  THIRD MESSAGE OF QUICK MODE ****
[2006-05-10 07:50:03]**** QUICK MODE COMPLETED ****
[2006-05-10 07:50:03][==== IKE PHASE 2 ESTABLISHED====]
```

L'état des connexions.

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	2563133384	marbriers	86.194.16	ESP	78	25070	25040
2	3568566769	INmarbriers	172.16.1.14	ESP	181	25070	0

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	marbriers	86.194.16	SA_MATURE	25070

Ceci n'est pas un cryptage 3DES.

Sleon une édtue de l'Uvinertisé de Cmabrigde, l'odrre des ltteers dnas un mto n'a pas d'ipmrotncae, la suele coshe ipmrotnate est que la pmeirère et la drenèire soeint à la bnnoe pclae.

Et vcioi le txete en cialr.

Selon une étude de l'Université de Cambridge, l'ordre des lettres dans un mot n'a pas d'importance, la seule chose importante est que la première et la dernière soient à la bonne place.

Sources :
Les captures d'écran sont le reflet d'une installation réalisée sur Lyon.
Les explications techniques proviennent de Netgear et HSC consultant.