Serveur VPN avec des clients Windows

J'aime bien avoir accès à mes petites affaires quand je suis en déplacements (vacances, déplacements professionnels ou autres), et du coup, monter un VPN avec mon serveur c'est sympa.

OpenBSD permet de monter facilement des VPN en utilisant IPSec, chose assez agréable.

Surtout que la configuration prend environ 10 minutes...

Installation et configuration du service

Il faut d'abord modifier le fichier '`/etc/ipsec.conf`' comme suit :

```
ike passive from any to any \
        main auth hmac-sha1 enc aes group modp1024 \
        quick auth hmac-sha1 enc aes \
        psk "MonSuperSecret"
```

Alors non, ce n'est pas bien de mettre `from any to any` comme ça, il faudrait être plus restrictif.

Vous pouvez utilisez jot pour générer un “pre-shared secret”...

Dans le fichier '`/etc/pf.conf`' il faut ajouter ces lignes-là :

```
set skip on enc0
[... plus bas...]
# IPsec
pass in quick on egress inet proto udp to egress port { isakmp, ipsec-nat-t
} modulate state
pass quick on egress inet proto esp to egress
```

Alors non, ce n'est toujours pas bien : rien n'est filtré dans le tunnel (`skip on enc0`), et rien n'est filtré au niveau du protocole ESP non plus...

Enfin, histoire de rendre ça un petit peu permanent, il faut modifier le fichier '`/etc/rc.conf.local`' et ajouter :

```
isakmpd_flags="-K"
ipsec=""
```

Lancement manuel

Pour tester tout ça, il faut lancer les sevices à la main :

```
isakmpd -K
```

```
ipsecctl -f /etc/ipsec.conf
```

Configuration des clients

Des gens bien informés utilisent Shrew Soft VPN Client pour faire du VPN sous Windows.

Bin moi je fais pareil du coup.

Après avoir installé le logiciel, le lancer et créer une nouvelle connexion.

Dans l'onglet “Général”, entrez l'IP publique de votre serveur (une IP fixe, c'est mieux... à défaut un service type DynDNS c'est sympa), choisissez “Use a virtual adaptor and assigned IP” et entrez une IP valide de votre réseau et pas une affectée par le DHCP de préférence...) ainsi que son masque réseau.

Dans l'onglet “Name Resolution”, entrez l'IP privée de votre serveur et désactivez le serveur WINS.

Dans l'onglet “Authentication”, choisissez “Mutual PSK” et l'identification “IP Address” dans les sous-onglets “Local Identity” et “Remote Identity”. Enfin, dans le dernier sous-onglet, “Credentials”, entrez la même chose que le `psk` du fichier `'/etc/ipsec.conf'` du serveur.

Dans l'onglet “Phase 1”, choisissez “group 2” pour “DH Exchange”.

Dans l'onglet “Phase 2”, choisissez “group 2” pour “PSF Exchange”.

Ne changez rien dans les autres onglets.

Vous pouvez ensuite lancer la connexion qui doit s'établir toute seule... :)

A vous les joies de pouvoir accéder à vos partages Samba et tout le reste depuis un endroit distant. A une vitesse folle : vive l'ADSL !

Cas d'un serveur avec une IP publique dynamique

Bin oui, des fois ça arrive, si vous n'êtes pas chez Free par exemple.

Dans ce cas, il vous faudra pouvoir obtenir automatiquement votre IP à chaque renouvellement. Moi j'ai choisi de m'envoyer un mail (sur une boite externe, genre gmail ou autre) avec la nouvelle IP.

Il ne vous restera plus qu'à modifier la configuration de votre client pour pouvoir établir votre connexion.

Voici mon script :

get-ip.sh

```
#!/bin/ksh

WDIR=/root/DynIP
```

```
IP=$(ftp -o - http://free-unices.org/home/your_ip.php 2>/dev/null |
head -1 | cut -d':' -f2)

[[ -z "$IP" ]] && exit

if [ -e ${WDIR}/old_ip ]; then
  OLD_IP=$(cat ${WDIR}/old_ip)
  if [ "$IP" = "$OLD_IP" ]; then
    exit
  else
    echo "$IP" > ${WDIR}/old_ip
  fi
else
  echo "$IP" > ${WDIR}/old_ip
fi

echo "New IP address is: $IP"

exit

# EoF
```

Je trouve mon IP sur mon site web, compare avec l'ancienne IP, et affiche la nouvelle, la cas échéant. Pour diverses raisons (la principale étant que je modifiais une zone DNS dynamique avant, quand j'étais grand et velu), je lance ce script en root, et c'est le mal. Mais c'est historique, alors ça va. Ou en tout cas c'est comme ça dans le merveilleux monde du travail, alors pourquoi pas chez moi ?

Enfin, je lance ce script toutes les 10 minutes grâce à `cron` (et tout ce que mon planificateur affiche est envoyé à une adresse mail, normal non ?).