```
###################################
###################################
## OpenVPN - Installation Serveur ##
###################################
###################################
```

```
################
# Présentation #
################
```

Cette technique permet la création d'une liaison chiffrée entre votre machine et un serveur hébergé sur Internet (par exemple chez un fournisseur d'accès se trouvant en France ou à l'étranger). Tous vos accès à Internet seront alors vus à partir de l'adresse IP de ce serveur VPN et non plus par celle de votre machine.

OpenVPN n'est pas un VPN IPSec. C'est un VPN se basant sur la création d'un tunnel IP (UDP ou TCP au choix) authentifié et chiffré avec la bibliothèque OpenSSL.

Quelques avantages des tunnels VPN :
- Facilité pour passer les réseaux NATés (pas de configuration à faire)
- Logiciel clients disponibles sur GNU/Linux, BSD, Windows et Mac OS X

```
################
# Installation #
################
```

On commence par installer OpenVPN à partir des dépôts officiels :

Pour Debian :

```
aptitude install openvpn zip
```

Pour Archlinux :

```
pacman -S openvpn zip
```

On copie ensuite les fichiers de configurations :

```
mkdir /etc/openvpn/easy-rsa/
cp -r /usr/share/doc/openvpn/examples/easy-rsa/2.0/* /etc/openvpn/easy-rsa/
chown -R $USER /etc/openvpn/easy-rsa/
```

```
#################
# Configuration #
#################
```

À l'aide des scripts installés dans le répertoire */etc/openvpn/easy-rsa/* nous allons configurer OpenVPN pour utiliser une authentification par clés et certificats.

On commence par éditer le fichier */etc/openvpn/easy-rsa/vars* :

```
export KEY_COUNTRY="FR"
export KEY_PROVINCE="FR"
export KEY_CITY="FR"
export KEY_ORG="exemple.com"
export KEY_EMAIL="exemple@exemple.com"
```

Ensuite on lance la séquence suivante qui va générer les clés (.key) et les certificats (.crt) :

```
cd /etc/openvpn/easy-rsa/
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
```

openvpn --genkey --secret keys/ta.key

On copie ensuite les clés et les certificats utiles pour le serveur dans le répertoire */etc/openvpn/* :

cp keys/ca.crt keys/ta.key keys/server.crt keys/server.key keys/dh1024.pem /etc/openvpn/

Puis on génère un répertoire */etc/openvpn/jail* dans lequel le processus OpenVPN sera chrooté (afin de limiter les dégâts en cas de faille dans OpenVPN) puis un autre répertoire */etc/openvpn /clientconf* qui contiendra la configuration des clients :

mkdir /etc/openvpn/jail
mkdir /etc/openvpn/clientconf

Enfin on crée le fichier de configuration */etc/openvpn/server.conf* :

```
# Serveur TCP/443
mode server
proto tcp
port 443
dev tun

# Clés et certificats
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
tls-auth ta.key 0
cipher AES-256-CBC

# Réseau
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
keepalive 10 120

# Sécurite
user nobody
group nogroup
chroot /etc/openvpn/jail
persist-key
persist-tun
comp-lzo

# Log
verb 3
mute 20
status openvpn-status.log
log-append /var/log/openvpn.log
```

Ce fichier permet de créer un serveur VPN SSL routé basé sur le protocole TCP et utilisant le port HTTPS (443) afin de maximiser son accessibilité depuis des réseaux sécurisés par des Firewalls. Les clients obtiendront une nouvelle adresse IP dans le range 10.8.0.0/24.

########################
Démarrage du serveur
########################

On lance le serveur avec la commande :

/etc/init.d/openvpn start

À ce stade les machines clientes vont pouvoir se connecter au serveur VPN. Par contre impossible d'aller plus loin que ce dernier car l'adresse 10.8.0.x ne sera par routée en dehors de votre serveur. Il faut donc configurer le serveur pour qu'il joue le rôle de routeur entre l'interface VPN (tun0) et l'interface physique (eth0) et de NATeur entre les adresses en 10.8.0.x et son

adresse IP réelle.

Configuration du routage :

sh -c 'echo 1 > /proc/sys/net/ipv4/ip_forward'

Pour rendre ce paramètrage de routage permanent (même après un reboot), il faut ajouter la ligne suivante au fichier */etc/sysctl.conf* :

net.ipv4.ip_forward = 1

Puis configurer la translation d'adresse (NAT) :

iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o eth0 -j MASQUERADE

Pour rendre cette règle de NAT persistante après un reboot de votre serveur, il faut commencer par créer un script de chargement de règles de Firewall (ou utiliser un script existant) :

sh -c "iptables-save > /etc/iptables.rules"

Le serveur est maintenant prêt à accueillir les clients.

##################################
##################################
OpenVPN - Installation Client
##################################
##################################

################
Installation
################

Pour Debian :

aptitude install openvpn

Pour Archlinux :

pacman -S openvpn

################
Configuration
################

Nous allons créer les clés pour le client "client1", pour cela il faut saisir les commandes suivantes sur le serveur :

cd /etc/openvpn/easy-rsa source vars ./build-key client1

Si vous souhaitez protéger l'accès à vos clés par un mot de passe (c'est à dire qu'un mot de passe sera demandé à la montée du tunnel VPN), il faut utiliser la commande **./build-key-pass** en lieu et place de **./buil-key.**

Le script **./build-key** va générer 3 fichiers dans le répertoire */etc/openvpn/easy-rsa/keys* :

client1.crt: Certificat pour le client
client1.csr: Certificat à garder sur le serveur
client1.key: Clés pour le client

On copie les fichiers nécessaires dans un sous répertoire du répertoire */etc/openvpn/clientconf/* préalablement crée :

mkdir /etc/openvpn/clientconf/client1/
cp /etc/openvpn/ca.crt /etc/openvpn/ta.key keys/client1.crt keys/client1.key /etc/openvpn /clientconf/client1/

On va ensuite dans le répertoire */etc/openvpn/clientconf/client1/* :

cd /etc/openvpn/clientconf/client1/

Puis on créé le fichier *client.conf* (il faut remplacer **A.B.C.D** par l'adresse publique de votre serveur VPN :

```
# Client
client
dev tun
proto tcp-client
remote A.B.C.D 443
resolv-retry infinite
cipher AES-256-CBC

# Clés
ca ca.crt
cert client1.crt
key client1.key
tls-auth ta.key 1

# Sécurite
nobind
persist-key
persist-tun
comp-lzo
verb 3
```

Pour assurer la compatibilité avec le client Windows OpenVPN, on fait une copie du fichier *client.conf* vers *client.ovpn* :

cp client.conf client.ovpn

On devrait ainsi avoir les fichiers suivants dans le répertoire */etc/openvpn/clientconf/client1/* :

```
ca.crt: Certificat du serveur
client.conf: Fichier de configuration du client OpenVPN (Linux, BSD, MacOS X)
client.ovpn: Fichier de configuration du client OpenVPN (Windows)
client1.crt: Certificat du client
client1.key: Clés du client
ta.key: Clés pour l'authentification
```

Il ne reste plus qu'à mettre ces fichiers dans une archive ZIP et de la transmettre sur le PC client :

zip client1.zip *.*

###########
Accueil
###########