OPENVPN Serveur et Client

- Objet : du tuto Configuration d'un serveur openvpn
- Niveau requis :
  avisé
- Commentaires : *serveur, nat..*
- Suivi :
  - Création par kawer 18/12/2018
  - Testé par kawer le 18/12/2018
- Commentaires sur le forum : Lien vers le forum concernant ce tuto [1)]

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 SSL 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 SSL :

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

Partie Serveur

Installation Sur le Serveur

On commence par installer OpenVPN à partir des dépôts officiels :

```
apt-get update && apt-get install openvpn easy-rsa
```

On se prépare à installer les certificats

```
cd /etc/openvpn
```

```
make-cadir nom_du_serveur
```

```
cd /etc/openvpn/nom_du_serveur
```

```
ln -s openssl-1.0.0.cnf openssl.cnf
```

```
nano /etc/openvpn/nom_du_serveur/vars
```

Ce qui donne par exemple :

```
export KEY_SIZE=4096 # Une clef de 4096 est le minimum actuellement pour un
chiffrement correct
export KEY_COUNTRY="EU"
export KEY_PROVINCE="FR"
export KEY_CITY="Paris"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@debian-facile.org"
export KEY_OU="MyOrganizationalUnit"
export KEY_NAME="nom_du_serveur_vpn" # Choisissez un nom dont vous vous
souviendrez !
```

Génération des clefs RSA 4096 :

```
cd /etc/openvpn/nom_du_serveur
```

```
source ./vars
```

on applique toutes les variables edité précedement.

```
./clean-all
```

Faite gaffe en utilisant cette commande, elle efface toutes les cléfs si vous en avez déjà créée.

```
./build-ca
```

Création du certificat d'authorité du serveur

```
./build-key-server nom_du_serveur
```

Ce qui donne par exemple à la fin :

```
A challenge password []:votre_mot_de_passe
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
```

```
openvpn --genkey --secret /etc/openvpn/nom_du_serveur/keys/ta.key
```

```
cd /etc/openvpn/nom_du_serveur
```

```
openssl dhparam 4096 > keys/dh-4096.pem
```

Configuration de base côté serveur :

```
gunzip -c /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
> /etc/openvpn/nom_du_serveur.conf
```

```
nano /etc/openvpn/nom_du_serveur.conf
```

#Attention, les ';' sont là pour désactiver les options

En plus des informations déjà présente, et celle si comprise, vous devez modifier/ajouter les lignes suivantes, à adapter selon votre cas :

```
port 7777
proto tcp
;proto udp
ca /etc/openvpn/nom_du_serveur/keys/ca.crt
cert /etc/openvpn/nom_du_serveur/keys/nom_du_serveur.crt
key /etc/openvpn/nom_du_serveur/keys/nom_du_serveur.key  # This file should
be kept secret
dh /etc/openvpn/nom_du_serveur/keys/dh-4096.pem
tls-auth /etc/openvpn/nom_du_serveur/keys/ta.key 0 # This file is secret
cipher AES-256-CBC
auth SHA512
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-
DHE-RSA-WITH-AES-256-CBC-SHA:TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA:TLS-DHE-
RSA-WITH-AES-128-CBC-SHA:TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA
comp-lzo
user openvpn
group nogroup
;explicit-exit-notify 1
```

Création de l'utilisateur openvpn :

```
adduser --system --shell /usr/sbin/nologin --no-create-home openvpn

=== Test et Démarrage du serveur : ===

<code root>openvpn /etc/openvpn/nom_du_serveur.conf
```

Si vous obtenez “Initialization Sequence Completed” en dernière ligne alors passez à la commande suivante, sinon ouvrez un post dans la rubrique réseau du forum.

```
systemctl start openvpn
```

```
systemctl start openvpn@nom_du_serveur
```

```
systemctl enable openvpn
```

```
systemctl enable openvpn@nom_du_serveur
```

Génération des clients sur le serveur :

```
cd /etc/openvpn/nom_du_serveur
```

```
source ./vars
```

```
./build-key nom_du_client
```

A la fin des options à saisir :

```
A challenge password []:votre_mot_de_passe_précédement_créée
Sign the certificate? [y/n]:y
1 out of 1 certificate requests certified, commit? [y/n]y
```

Configuration reseau

Activation de l'ip forwarding pour le NAT :

```
echo "net.ipv4.ip_forward=1" > /etc/sysctl.d/NAT.conf
```

Activez le nouveau jeux de règle :

```
sysctl -p /etc/sysctl.d/NAT.conf
```

Quelques explications concernant la configuration du NAT sur le forum ici merci à raleur pour ces explications :)

Ajouts des règles dans iptables :

se référer ici : tuto Reseau iptable

```
iptables -t filter -P FORWARD ACCEPT
iptables -t filter -A INPUT -p tcp --dport 7777 -j ACCEPT
iptables -t nat -A POSTROUTING -o ethx(nom de votre interface) -j MASQUERADE
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o ethx(nom de votre
interface) -j MASQUERADE
```

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

```
iptables-save > /etc/iptables.rules
```

Instalation Sur le Client

On installe openvpn :

```
sudo apt-get update
```

```
sudo apt-get install openvpn
```

Configuration d'openvpn :

```
mkdir -p /etc/openvpn/nom_du_serveur/clients
```

```
cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
/etc/openvpn/nom_du_serveur/clients/nom_du_client.ovpn
```

```
nano /etc/openvpn/nom_du_serveur/clients/nom_du_client.ovpn
```

Doit y être ajouté et ou modifié les lignes suivantes :

```
proto tcp
;proto udp
remote ip_du_serveur 7777
user nobody
group nogroup
ca ca.crt
cert nom_du_client.crt
key nom_du_client.key
tls-auth ta.key 1
cipher AES-256-CBC
auth SHA512
TLS-DHE-RSA-WITH-AES-256-GCM-SHA384:TLS-DHE-RSA-WITH-AES-128-GCM-SHA256:TLS-
DHE-RSA-WITH-AES-256-CBC-SHA:TLS-DHE-RSA-WITH-CAMELLIA-256-CBC-SHA:TLS-DHE-
RSA-WITH-AES-128-CBC-SHA:TLS-DHE-RSA-WITH-CAMELLIA-128-CBC-SHA
comp-lzo
```

On récupère les certificats sur le serveur :

Rappatriez ca.crt nom_du_client.crt nom_du_client.key et ta.key de /etc/openvpn/nom_du_serveur/keys sur votre client dans /etc/openvpn/nom_du_serveur/nom_du_client/ scp : transfert de fichiers sécurisé entre machines

Déconseillé d'utiliser la connexion via le compte root à travers internet!! Pour bien faire il faut mettre tout ça dans un répertoire, le compresser via targz, lui donner les droits d'un user qui est sur le client et enfin récupérer cette archive à partir du client

via le user avec scp...

Tester la configuration :

```
cd /etc/openvpn/nom_du_server/nom_du_client
```

```
openvpn nom_du_client.ovpn
```

#Vous devriez obtenir 'Initialization Sequence Completed' dans le cas contraire ouvrez un post dans la rubrique reseau

Il vous reste plus qu'a enable et start openvpn et openvpn@nom_du_client de la même façon que sur le serveur.

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !