OPENVPN Serveur et Client

- Objet : du tuto Configuration d'un serveur openvpn
- Niveau requis :
  avisé
- Commentaires : *serveur, nat..*
- Suivi :
  - Création par kawer 27/05/2016
  - Testé par Tsukasa le 22/01/2017
- 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**

Installation

On commence par installer OpenVPN à partir des dépôts officiels :

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

On se prépare à installer les certificats

```
cp -a /usr/share/easy-rsa /etc/openvpn/
```

```
cd /etc/openvpn/easy-rsa
```

```
source vars
```

```
./clean-all
```

Création des certificats de l'autorité de certification :

sur stretch et buster easy-rsa ne trouve pas le fichier openssl.cnf dans /etc/openvpn/easy-rsa Il faut créer un lien symbolique qui pointe vers le fichier le plus récent présent dans ls -l /etc/openvpn/easy-rsa et qui est openssl-1.0.0.cnf à ce jour

Pour créer le lien il faut se rendre dans le bon répertoire:

```
cd /etc/openvpn/easy-rsa
```

puis faire le lien symbolique:

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

```
./build-ca
```

Vous devriez obtenir ce qui suit, libre à vous d'en changer le contenus :

```
Generating a 2048 bit RSA private key
................++++
.....................................................................................
.....................................................................................
....+++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:
```

On génère la clé Diffie-Hellman qui sert à sécuriser les échanges :

```
./build-dh
```

Qui donne :

```
Generating DH parameters, 2048 bit long safe prime, generator 2
This is going to take a long time
..............+.....................................................
.......................
```

On génère les certificats du serveur :

```
./build-key-server srvcert
```

Qui donne ce qui suit : **(remplacez debian-facile par le nom de votre serveur)**

```
Generating a 2048 bit RSA private key
....+++
................................+++
writing new private key to 'srvcert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname) [srvcert]:debian-
facile
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'debian-facile'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'me@myhost.mydomain'
```

```
Certificate is to be certified until Jun 19 19:40:11 2025 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Création du fichier de configuration pour le serveur

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

On configure server.conf

```
nano /etc/openvpn/server.conf
```

décommentez ou ajoutez les lignes suivantes :

```
#On limite les droits à l'utilisateur nobody et au groupe nogroup. Attention
cela n'est bon que pour les clients qui sont sur linux/unix.
#Pour les clients windows il faut commenter ces deux lignes
user nobody
group nogroup
---
#On limite le nombres de client simultanées
max-clients 5
---
#On active la compression ça permet de gagner de la bande passante et la
vitesse pour tout ce qui est binaire.
#Attention il faut aussi que cette ligne soit dans le fichier de
configuration du client openvpn
comp-lzo
---
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/srvcert.crt
key /etc/openvpn/easy-rsa/keys/srvcert.key  # This file should be kept
secret
---
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
---
push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
```

remplacez 8.8.8.8 et 8.8.4.4 par vos dns favoris)

On test la configuration openvpn pour le serveur:

```
service openvpn stop
```

```
openvpn /etc/openvpn/server.conf
```

Vous devriez obtenir quelque chose comme suit :

```
Thu Dec 22 18:27:00 2016 OpenVPN 2.3.4 x86_64-pc-linux-gnu [SSL (OpenSSL)]
[LZO] [EPOLL] [PKCS11] [MH] [IPv6] built on Nov 12 2015
Thu Dec 22 18:27:00 2016 library versions: OpenSSL 1.0.1t  3 May 2016, LZO
2.08
Thu Dec 22 18:27:00 2016 Diffie-Hellman initialized with 2048 bit key
Thu Dec 22 18:27:00 2016 Socket Buffers: R=[212992->131072]
S=[212992->131072]
Thu Dec 22 18:27:00 2016 ROUTE_GATEWAY 213.32.16.1
Thu Dec 22 18:27:00 2016 TUN/TAP device tun0 opened
Thu Dec 22 18:27:00 2016 TUN/TAP TX queue length set to 100
Thu Dec 22 18:27:00 2016 do_ifconfig, tt->ipv6=0,
tt->did_ifconfig_ipv6_setup=0
Thu Dec 22 18:27:00 2016 /sbin/ip link set dev tun0 up mtu 1500
Thu Dec 22 18:27:00 2016 /sbin/ip addr add dev tun0 local 10.8.0.1 peer
10.8.0.2
Thu Dec 22 18:27:00 2016 /sbin/ip route add 10.8.0.0/24 via 10.8.0.2
Thu Dec 22 18:27:00 2016 GID set to nogroup
Thu Dec 22 18:27:00 2016 UID set to nobody
Thu Dec 22 18:27:00 2016 UDPv4 link local (bound): [undef]
Thu Dec 22 18:27:00 2016 UDPv4 link remote: [undef]
Thu Dec 22 18:27:00 2016 MULTI: multi_init called, r=256 v=256
Thu Dec 22 18:27:00 2016 IFCONFIG POOL: base=10.8.0.4 size=62, ipv6=0
Thu Dec 22 18:27:00 2016 IFCONFIG POOL LIST
Thu Dec 22 18:27:00 2016 Initialization Sequence Completed
```

```
ifconfig tun0
```

Devrait vous retourner :

```
tun0      Link encap:UNSPEC  HWaddr
00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          inet addr:10.8.0.1  P-t-P:10.8.0.2  Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B
```

Le test s'est bien déroulé :

```
service openvpn start
```

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 udp --dport 1194 -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
```

Génération des certificats pour le client (oui nous sommes toujours sur le serveur)

```
cd /etc/openvpn/easy-rsa/
```

```
source vars
```

```
./build-key clientCert
```

Qui donne ce qui suit : **(remplacez [clientCert]:debianFacile par le nom de votre client)**

```
Generating a 2048 bit RSA private key
.........................................+++
.....................................................+++
```

```
writing new private key to 'monlaptopcert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [CA]:
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [MyOrganizationalUnit]:
Common Name (eg, your name or your server's hostname)
[clientCert]:debianFacile
Name [EasyRSA]:
Email Address [me@myhost.mydomain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /etc/openvpn/easy-rsa/openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'US'
stateOrProvinceName   :PRINTABLE:'CA'
localityName          :PRINTABLE:'SanFrancisco'
organizationName      :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'
commonName            :PRINTABLE:'debianFacile'
name                  :PRINTABLE:'EasyRSA'
emailAddress          :IA5STRING:'me@myhost.mydomain'
Certificate is to be certified until Jun 19 20:05:45 2025 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

openvpn comme client sur le poste client

On installe openvpn :

```
sudo apt-get update
```

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

On récupère les certificats sur le serveur :

Récupérer les fichiers suivant dans /etc/openvpn/easy-rsa/keys/: 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...

```
scp root@ip_du_serveur:/etc/openvpn/easy-rsa/keys/ca.crt /tmp/
```

```
scp root@ip_du_serveur:/etc/openvpn/easy-rsa/keys/clientCert.key /tmp/
```

```
scp root@ip_du_serveur:/etc/openvpn/easy-rsa/keys/clientCert.crt /tmp/
```

On copie le fichier de configuration et certificats

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

```
cd /etc/openvpn
```

```
mkdir -p keys
```

```
cd keys
```

Coller dans le dossiers en cours (keys) les fichiers suivants :

```
mv /tmp/ca.crt /etc/openvpn/keys/
```

```
mv /tmp/clientCert.key /etc/openvpn/keys/
```

```
mv /tmp/clientCert.crt /etc/openvpn/keys/
```

Modification du fichier de configuration sur le client

Changer le chemin du serveur et des certificats dans /etc/openvpn/client.conf

```
remote monServeurOpenVPN 1194
ca /etc/openvpn/keys/ca.crt
cert /etc/openvpn/keys/clientCert.crt
```

```
key /etc/openvpn/keys/clientCert.key
#On active la compression ça permet de gagner de la bande passante et la
vitesse pour tout ce qui est binaire.
#Attention il faut aussi que cette ligne soit dans le fichier de
configuration du serveur openvpn
comp-lzo
```

Pour que toutes les connexions passent par votre vpn il faut également ajouter:

```
redirect-gateway def1
```

Changez les DNS de votre client, ceux de votre FAI sont fermé! Vous pouvez utiliser ceux de opennic par exemple

Si vous utilisez Network-Manager c'est dans ces options que vous devez définir les nouveaux DNS à utiliser.Vous pouvez également le faire en ligne de commande:

```
nmcli con mod lenom-de-votre-connexion ipv4.dns "169.239.202.202
185.121.177.177"
```

Test de connection

```
openvpn /etc/openvpn/client.conf
```

Vous devez obtenir en fin de séquence :

```
Initialization Sequence Completed
```

Si tel est le cas, vérifiez que tun0 est bien listé avec **ifconfig**, puis vérifiez votre ip par exemple en allant sur http://ifconfig.me/, si tout est ok, on ferme la console openvpn en pensant a faire un **Ctrl+C**

on démarre openvpn

```
service openvpn start
```

[1)]

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