

TP OpenVPN



I- Configuration du serveur

Installation des paquets nécessaires :

apt-get install iptables-persistent openvpn openssl easy-rsa

Génération des certificats et clefs avec Openvpn :

- Copie du répertoire easy-rsa : cp -R /usr/share/easy-rsa/ /etc/openvpn/server
- On se place dans le répertoire server : cd /etc/openvpn/server/easy-rsa
- Modification du fichier vars : nano vars

```
export KEY_COUNTRY="FR"
export KEY_PROVINCE="Nord"
export KEY_CITY="Cambrai"
export KEY_ORG="SaintLuc"
export KEY_EMAIL="lefort.enzo59@gmail.com"
export KEY_OU="MonOrganisation"
```

- Véeification de la configuration SSL : ln -s openssl-x.x.x.cnf openssl.cnf
Vérifier la présence de /etc/openvpn/server/openssl.cnf
Si le fichier openssl.cnf est absent, mais que que plusieurs fichiers openssl-x.x.x.cnf
Alors on crée un lien vers la dernière version

- On recharge le paramétrage : ../vars et ./clean-all

```
root@Debian:/etc/openvpn/server/easy-rsa# ../vars
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/server/easy-rsa/keys
root@Debian:/etc/openvpn/server/easy-rsa# ./clean-all
```

- Génération d'une clef : ./build-ca

```
root@Debian:/etc/openvpn/server/easy-rsa# ./build-ca
Generating a 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) [FR]:
State or Province Name (full name) [Nord]:
Locality Name (eg, city) [Cambrai]:
Organization Name (eg, company) [SaintLuc]:
Organizational Unit Name (eg, section) [MonOrganisation]:
Common Name (eg, your name or your server's hostname) [SaintLuc CA]:
Name [EasyRSA]:
Email Address [lefort.enzo59@gmail.com]:
```

Génération du certificat et des clefs pour le Serveur :

- Génération de la clef pour le serveur : ./build-key-server server

```
.....+++++
writing new private key to 'server.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) [FR]:
State or Province Name (full name) [Nord]:
Locality Name (eg, city) [Cambrai]:
Organization Name (eg, company) [SaintLuc]:Organisation-SaintLuc
Organizational Unit Name (eg, section) [MonOrganisation]:
Common Name (eg, your name or your server's hostname) [server]:
Name [EasyRSA]:
Email Address [lefort.enzo59@gmail.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:sio-2018
An optional company name []:
Using configuration from /etc/openvpn/server/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'FR'
stateOrProvinceName     :PRINTABLE:'Nord'
localityName            :PRINTABLE:'Cambrai'
organizationName        :PRINTABLE:'Organisation-SaintLuc'
organizationalUnitName  :PRINTABLE:'MonOrganisation'
commonName              :PRINTABLE:'server'
name                    :PRINTABLE:'EasyRSA'
emailAddress            :IA5STRING:'lefort.enzo59@gmail.com'
Certificate is to be certified until Dec 14 10:46:04 2029 GMT (3650 days)
Sign the certificate? [y/n]:_

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
```

- Génération de la clef pour le client : ./build-key client1

```
.....+++++
writing new private key to 'client1.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) [FR]:
State or Province Name (full name) [Nord]:
Locality Name (eg, city) [Cambrai]:
Organization Name (eg, company) [SaintLuc]:
Organizational Unit Name (eg, section) [MonOrganisation]:
Common Name (eg, your name or your server's hostname) [client1]:
Name [EasyRSA]:
Email Address [lefort.enzo59@gmail.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:sio2018
An optional company name []:
Using configuration from /etc/openvpn/server/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'FR'
stateOrProvinceName     :PRINTABLE:'Nord'
localityName            :PRINTABLE:'Cambrai'
organizationName        :PRINTABLE:'SaintLuc'
organizationalUnitName  :PRINTABLE:'MonOrganisation'
commonName              :PRINTABLE:'client1'
name                    :PRINTABLE:'EasyRSA'
emailAddress            :IA5STRING:'lefort.enzo59@gmail.com'
Certificate is to be certified until Dec 14 10:48:15 2029 GMT (3650 days)
Sign the certificate? [y/n]:
```

```
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
```

Pour les autres clients : : ./build-key client2 etc...

- Génération du paramètre dh : ./build-dh

[illegible]

- Pour voir le résultat : `vdir`

```

root@Debian:/etc/openvpn/server/easy-rsa# vdir
total 116
-rwxr-xr-x 1 root root 119 déc. 17 09:33 build-ca
-rwxr-xr-x 1 root root 352 déc. 17 09:33 build-dh
-rwxr-xr-x 1 root root 188 déc. 17 09:33 build-inter
-rwxr-xr-x 1 root root 163 déc. 17 09:33 build-key
-rwxr-xr-x 1 root root 157 déc. 17 09:33 build-key-pass
-rwxr-xr-x 1 root root 249 déc. 17 09:33 build-key-pkcs12
-rwxr-xr-x 1 root root 268 déc. 17 09:33 build-key-server
-rwxr-xr-x 1 root root 213 déc. 17 09:33 build-req
-rwxr-xr-x 1 root root 158 déc. 17 09:33 build-req-pass
-rwxr-xr-x 1 root root 449 déc. 17 09:33 clean-all
-rwxr-xr-x 1 root root 1471 déc. 17 09:33 inherit-inter
drwx----- 2 root root 4096 déc. 17 11:51 keys
-rwxr-xr-x 1 root root 302 déc. 17 09:33 list-crl
-rw-r--r-- 1 root root 7859 déc. 17 09:33 openssl-0.9.6.cnf
-rw-r--r-- 1 root root 8416 déc. 17 09:33 openssl-0.9.8.cnf
-rw-r--r-- 1 root root 8313 déc. 17 09:33 openssl-1.0.0.cnf
lrwxrwxrwx 1 root root 17 déc. 17 09:36 openssl.cnf -> openssl-1.0.0.cnf
-rwxr-xr-x 1 root root 13192 déc. 17 09:33 pkitool
-rwxr-xr-x 1 root root 1035 déc. 17 09:33 revoke-full
-rwxr-xr-x 1 root root 178 déc. 17 09:33 sign-req
-rw-r--r-- 1 root root 2070 déc. 17 09:35 vars
-rwxr-xr-x 1 root root 740 déc. 17 09:33 whichopensslcnf

```

Configuration du serveur :

- Copie du répertoire contenant les clefs : `cp -R /etc/openvpn/server/easy-rsa/keys/ /etc/openvpn`

```
root@Debian:/etc/openvpn/server/easy-rsa# cd /etc/openvpn
root@Debian:/etc/openvpn# ls
client ipp.txt keys openvpn-status.log server server.conf update-resolv-conf
root@Debian:/etc/openvpn#
```

- Création du fichier de configuration du serveur : nano /etc/openvpn/server.conf

```
GNU nano 2.7.4 Fichier : /etc/openvpn/server.conf
#Port protocole et interface
port 1194
proto udp
dev tun

#Chemin vers les fichiers ssl
ca keys/ca.crt
cert keys/server.crt
key keys/server.key
dh keys/dh2048.pem

#IP désirée pour le serveur
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"
push "dhcp-option DNS 10.8.0.1"
persist-key
persist-tun
comp-lzo

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

- Configuration de IPTABLES : (changer enp0s3 par le nom de votre carte réseau et l'adresse IP)
iptables -A INPUT -i enp0s3 -p udp -m udp --dport 1194 -j ACCEPT
iptables -A FORWARD -i tun0 -o enp0s3 -j ACCEPT
iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o enp0s3 -j MASQUERADE
- Activer le forwarding : echo 1 > /proc/sys/net/ipv4/ip_forward
 L'ip_forwarding ne sera pas conservé au prochain démarrage, il faudra éditer le fichier /etc/sysctl.conf et dé-commenter la ligne suivante : net.ipv4.ip_forward=1

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Lancer le serveur :

- cd /etc/openvpn
openvpn server.conf
- Lancer le serveur : service openvpn start

```
root@Debian:/etc/openvpn# service openvpn start
```

II- Configuration du client

Installation du paquet nécessaires :

apt-get install openvpn

- Récupération des fichiers ca.crt, client1.crt et client1.key sur le serveur via sftp (par exemple) dans :
cd /etc/openvpn/keys
- On met les fichiers récupérés sur le client dans le dossier dans : cd /etc/openvpn

```
root@Debian:/etc/openvpn# ls
ca.crt  client  client1.conf  client1.crt  client1.key  server  update-resolv-conf
```

- On crée un fichier client1.conf dans /etc/openvpn : nano /etc/openvpn/client1.conf

```
GNU nano 2.7.4 Fichier : /etc/openvpn/client1.conf

client
dev tun
proto udp
remote 172.16.0.1 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert eee.crt
key eee.key
comp-lzo
verb 3
pull
```

Lancer le client :

- cd /etc/openvpn
openvpn client1.conf

III- Test du service

En faisant `ip addr` nous pouvons voir qu'une nouvelle interface apparait, il s'agit du tunnel de notre VPN.

```
6: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN group default qlen 100
    link/none
    inet 10.8.0.1 peer 10.8.0.2/32 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::296a:2029:bb23:cc88/64 scope link flags 800
        valid_lft forever preferred_lft forever
```

Lancer le serveur :

- `cd /etc/openvpn`
`openvpn server.conf`
- Lancer le serveur : `service openvpn start`

Lancer le client :

- `cd /etc/openvpn`
`openvpn client1.conf`

Maintenant, depuis le serveur il sera possible de pinguer le client. Et depuis le client de pinguer le serveur et les machines du sous-réseau.

Depuis le client en allant sur ce lien <http://www.mon-ip.com/>, il est possible de connaître son IP et de voir le changement.

Index :

Pour résoudre cette erreur : *cannot load DH parameters from /etc/openvpn*

`openssl dhparam -out dh1024.pem 1024`