

# Mise en pratique : installation d'OpenVPN sur OpenWRT

OpenWRT est un système GNU/Linux open source conçu pour le matériel réseau (principalement des routeurs et points d'accès wi-fi) permettant l'ajout d'un myriade de fonctionnalités et améliorant celle déjà présentes.

## Installation d'OpenWRT sur un routeur TPLINK

Pour cela rien de plus simple il suffit de mettre à jour le firmware du routeur par l'image contenant OpenWRT via l'interface Web.

## Installation d'OpenVPN

Pour commencer je me suis connecté en SSH sur le routeur avec la commande « ssh 192.168.1.1 »

Ce qui suit est le retour SSH que j'ai commenté et annoté en **bleu** :

```
~~~~~ PuTTY log~~~~~
login as: root
root@192.168.1.1's password:
```

```
BusyBox v1.19.4 (2012-10-12 05:19:00 UTC) built-in shell (ash)
Enter 'help' for a list of built-in commands.
```

```
-----
|         | .----- .----- .----- . | | | | .----- |__|
|         | |  _   | _ _ |     | | | | | | _ _ | | |   |
|         | |__| W I R E L E S S   F R E E D O M
-----
```

-----  
ATTITUDE ADJUSTMENT (Attitude Adjustment, r33883)  
-----

```
* 1/4 oz Vodka      Pour all ingredients into mixing
* 1/4 oz Gin        tin with ice, strain into glass.
* 1/4 oz Amaretto
* 1/4 oz Triple sec
* 1/4 oz Peach schnapps
* 1/4 oz Sour mix
* 1 splash Cranberry juice
-----
```

```
root@OpenWrt:~# opkg update Mise à jour des dépôts de paquets
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09-
beta2/ar71xx/generic/packages/Packages.gz.
Inflating http://downloads.openwrt.org/attitude_adjustment/12.09-
beta2/ar71xx/generic/packages/Packages.gz.
Updated list of available packages in /var/opkg-
```

```
lists/attitude_adjustment.
root@OpenWrt:~# opkg install openvpn openvpn-easy-rsa Installation des
paquets
Installing openvpn (2.2.2-2) to root...
Downloading http://downloads.openwrt.org/attitude_adjustment/12.09-
beta2/ar71xx/generic/packages/openssl-util_1.0.1c-1_ar71xx.ipk.
Configuring kmod-tun.
Configuring zlib.
Configuring libopenssl.
Configuring openssl-util.
Configuring liblzo.
Configuring openvpn.
Configuring openvpn-easy-rsa.
root@OpenWrt:~# cd /etc/easy-rsa
root@OpenWrt:/etc/easy-rsa# vi vars
```

```
# OpenVPN package upgrade.
e.
on-to-be-created key    key
```

```
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-
rsa/keys
```

```
Generating a 1024 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]:FR
```

```
State or Province Name (full name) [CA]:Martinique           Marti           FWI
```

```
Locality Name (eg, city) [SanFrancisco]:Marin
```

```
Organization Name (eg, company) [Fort-Funston]:Infologeek
```

```
Organizational Unit Name (eg, section) [changeme]:Infologeek
```

```
Common Name (eg, your name or your server's hostname)
```

```
[changeme]:Infologeek
```

```
Name [changeme]:Infologeek
```

```
Email Address [mail@host.domain]:contact@infologeek.fr
```

```
root@OpenWrt:/etc/easy-rsa# build-dh Création de la clé privée
```

```
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-
rsa/keys
```

```
Generating DH parameters, 1024 bit long safe prime, generator 2
```

```
This is going to take a long time
```

```
.....+.....
```

```
+.....+.....+*+*+*+*+*
```

```
root@OpenWrt:/etc/easy-rsa# build-dh Création de la clé publique
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-
rsa/keys
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time
```

```
root@OpenWrt:/etc/easy-rsa# build-key-server server Création de la clé privée
RSA
```

```
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-
rsa/keys
```

```
Generating a 1024 bit RSA private key
```

```
.....+++++
.....+
+++++
```

```
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) [US]:FR
```

```
State or Province Name (full name) [CA]:FWI
```

```
Locality Name (eg, city) [SanFrancisco]:Marin
```

```
Organization Name (eg, company) [Fort-Funston]:Infologeek
```

```
Organizational Unit Name (eg, section) [changeme]:
```

```
Common Name (eg, your name or your server's hostname) [server]:
```

```
Name [changeme]:
```

```
Email Address [mail@host.domain]:
```

```
Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
```

```
A challenge password []:dgsd5Zds2Z4f6é
```

```
An optional company name []:
```

```
Using configuration from /etc/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:'FR'
```

```
stateOrProvinceName  :PRINTABLE:'FWI'
```

```
localityName         :PRINTABLE:'Marin'
```

```
organizationName     :PRINTABLE:'Infologeek'
```

```
organizationalUnitName:PRINTABLE:'changeme'
```

```
commonName           :PRINTABLE:'server'
```

```
name                 :PRINTABLE:'changeme'
```

```
emailAddress         :IA5STRING:'mail@host.domain'
```

```
Certificate is to be certified until May  4 05:41:24 2023 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
root@OpenWrt:/etc/easy-rsa# build-key client Création de la clé publique RSA
NOTE: If you run ./clean-all, I will be doing a rm -rf on /etc/easy-
rsa/keys
Generating a 1024 bit RSA private key
.....++++++
.....++++++
writing new private key to 'client.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]:FR
State or Province Name (full name) [CA]:FWI
Locality Name (eg, city) [SanFrancisco]:
Organization Name (eg, company) [Fort-Funston]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [client]:
Name [changeme]:
Email Address [mail@host.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:U85sd*z&d9
An optional company name []:
Using configuration from /etc/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:'FR'
stateOrProvinceName  :PRINTABLE:'FWI'
localityName         :PRINTABLE:'SanFrancisco'
organizationName     :PRINTABLE:'Fort-Funston'
organizationalUnitName:PRINTABLE:'changeme'
commonName           :PRINTABLE:'client'
name                 :PRINTABLE:'changeme'
emailAddress         :IA5STRING:'mail@host.domain'
Certificate is to be certified until May  4 05:41:55 2023 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

```

```
root@OpenWrt:/etc/easy-rsa# vi /etc/openvpn/openvpn.conf
édition du fichier de configuration OpenVPN
```

```
mode server
tls-server
```

```
### network options
port 1194
proto udp
dev tun
```

```
### Certificate and key files
ca /etc/easy-rsa/keys/ca.crt
cert /etc/easy-rsa/keys/server.crt
key /etc/easy-rsa/keys/server.key
dh /etc/easy-rsa/keys/dh1024.pem
```

```
server 10.0.0.0 255.255.255.0
push "redirect-gateway def1"
push "dhcp-option DNS 192.168.1.1" # Change this to your router's LAN IP
Address
client-to-client
```

```
### (optional) compression (Can be slow)
#comp-lzo 0
persist-key
persist-tun
```

```
verb 3
keepalive 10 120
log-append /var/log/openvpn/openvpn.log
```

```
vi /etc/config/firewall
```

```
config 'include'
option 'path' '/etc/firewall.user'
config 'rule'
option 'target' 'ACCEPT'
option 'name' 'VPN'
option 'src' 'wan'
option 'proto' 'udp'
option 'dest_port' '1194'
```

```
root@OpenWrt:/etc/easy-rsa# vi /etc/firewall.user
```

```
iptables -t nat -A prerouting_wan -p udp --dport 1194 -j ACCEPT
iptables -A input_wan -p udp --dport 1194 -j ACCEPT
iptables -I INPUT -i tun+ -j ACCEPT iptables -I FORWARD -i tun+ -j ACCEPT
iptables -I OUTPUT -o tun+ -j ACCEPT iptables -I FORWARD -o tun+ -j
ACCEPT
```

```
root@OpenWrt:/etc/init.d/openvpn start
```

```
Démarrage d'OpenVPN
```

```
root@OpenWrt:/etc/easy-rsa# /etc/init.d/openvpn enable
```

```
Autodémarrage d'OpenVPN
```

```
root@OpenWrt:/etc/easy-rsa# exit
```

```
Fin de la session SSH
```

# Configuration d'OpenVPN client sous linux

```
user@ubuntu:/mkdir ~/VirtualNet
user@ubuntu:/sudo apt-get install openvpn
user@ubuntu:/vi ~/VirtualNet/client.ovpn
client
tls-client
dev tun
proto udp
remote 192.168.1.1 1194 Server OpenVPN
resolv-retry infinite
nobind
ca ca.crt
cert client.crt
key client.key
dh dh1024.pem
#comp-lzo Desactivation de la compression des données
persist-tun
persist-key
verb 3
user@ubuntu:/
user@ubuntu:/
user@ubuntu:/
user@ubuntu:/
user@ubuntu:/
```