

# *Cryptographie-Sécurité Services*

## Mise en place d'un serveur OpenVPN sous Debian



Réalisé Par :

Yossra safi chetouan

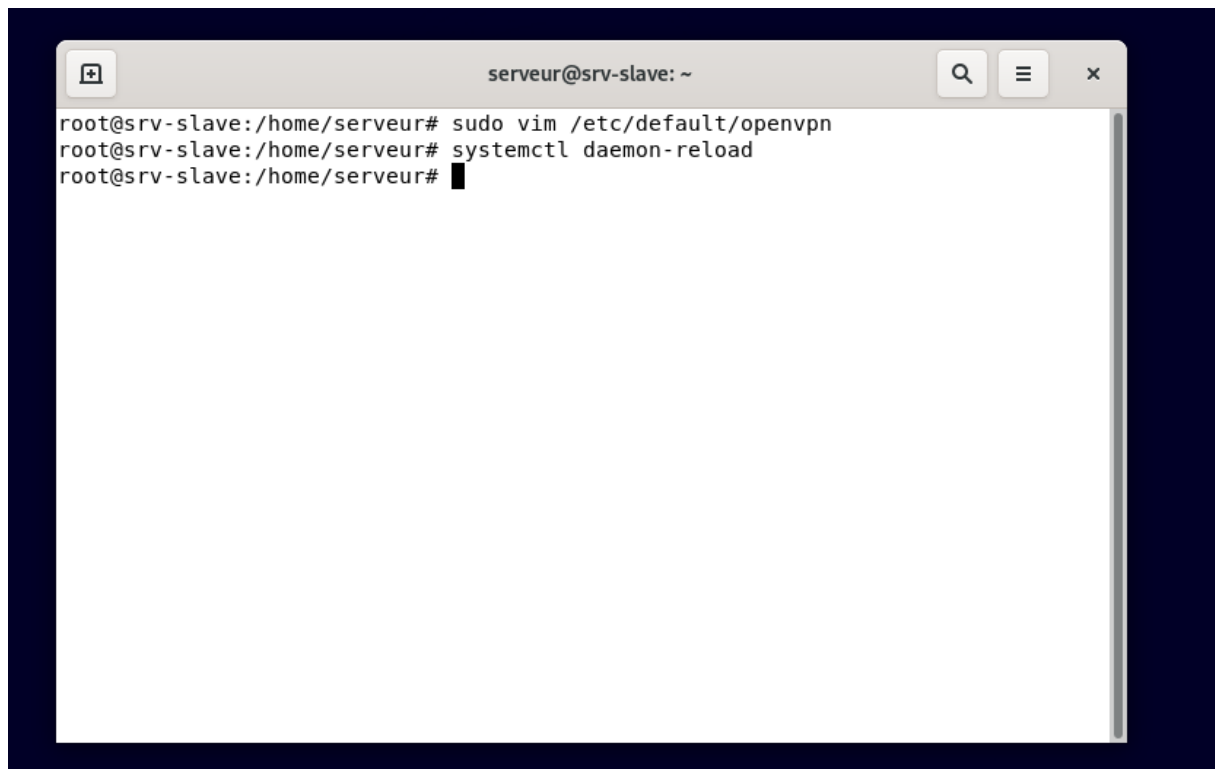
# 1. Configuration côté serveur Debian

## 1.1 Installation

```
serveur@srv-slave: ~  
root@srv-slave:/home/serveur# apt install openvpn  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  easy-rsa libccid libpkcs11-helper1 opensc opensc-pkcs11 pcscd  
Suggested packages:  
  pcmciautils resolvconf openvpn-systemd-resolved  
The following NEW packages will be installed:  
  easy-rsa libccid libpkcs11-helper1 opensc opensc-pkcs11 openvpn pcscd  
0 upgraded, 7 newly installed, 0 to remove and 5 not upgraded.  
Need to get 2,374 kB of archives.  
After this operation, 7,227 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y  
Get:1 http://deb.debian.org/debian bullseye/main amd64 libccid amd64 1.4.34-1 [37 kB]  
Get:2 http://deb.debian.org/debian bullseye/main amd64 pcscd amd64 1.9.1-1 [98.1 kB]  
Get:3 http://deb.debian.org/debian bullseye/main amd64 easy-rsa all 3.0.8-1 [45.2 kB]  
Get:4 http://deb.debian.org/debian bullseye/main amd64 libpkcs11-helper1 amd64 1.27-1 [47.5 kB]  
Get:5 http://deb.debian.org/debian bullseye/main amd64 opensc-pkcs11 amd64 0.21.0-1 [880 kB]
```

## 🔧 Activer OpenVPN au démarrage

```
serveur@srv-slave: ~  
# names of the VPNs. If empty, "all" is assumed.  
# The VPN name refers to the VPN configuration file name.  
# i.e. "home" would be /etc/openvpn/home.conf  
#  
# If you're running systemd, changing this variable will  
# require running "systemctl daemon-reload" followed by  
# a restart of the openvpn service (if you removed entries  
# you may have to stop those manually)  
#  
AUTOSTART="all"  
#AUTOSTART="none"  
#AUTOSTART="home office"  
#  
# WARNING: If you're running systemd the rest of the  
# options in this file are ignored.  
#  
# Refresh interval (in seconds) of default status files  
# located in /var/run/openvpn.$NAME.status  
# Defaults to 10, 0 disables status file generation  
#  
#STATUSREFRESH=10  
#STATUSREFRESH=0  
# Optional arguments to openvpn's command line  
-- INSERT --  
15,1 35%
```



A terminal window titled 'serveur@srv-slave: ~' with search, menu, and close buttons. The terminal shows the following commands and prompts:

```
root@srv-slave:/home/serveur# sudo vim /etc/default/openvpn
root@srv-slave:/home/serveur# systemctl daemon-reload
root@srv-slave:/home/serveur# █
```

## 1.2 Infrastructure à Clé Publique PKI (Public Key Infrastructure)

✚ Mise en place du pki :

```
serveur@srv-slave: ~  
root@srv-slave:/home/serveur# cd /etc/openvpn/  
root@srv-slave:/etc/openvpn# /usr/share/easy-rsa/easyrsa clean-all  
  
init-pki complete; you may now create a CA or requests.  
Your newly created PKI dir is: /etc/openvpn/pki  
  
root@srv-slave:/etc/openvpn# /usr/share/easy-rsa/easyrsa init-pki  
  
WARNING!!!  
  
You are about to remove the EASYRSA_PKI at: /etc/openvpn/pki  
and initialize a fresh PKI here.  
  
Type the word 'yes' to continue, or any other input to abort.  
Confirm removal:  
  
Aborting without confirmation.  
root@srv-slave:/etc/openvpn# █
```

✚ Création du certificate authority dans [/etc/openvpn/pki/ca.crt](#)

```
serveur@srv-slave: ~  
root@srv-slave:/etc/openvpn# /usr/share/easy-rsa/easyrsa build-ca nopass  
Using SSL: openssl OpenSSL 1.1.1w 11 Sep 2023  
Generating RSA private key, 2048 bit long modulus (2 primes)  
.....+++++  
.....+++++  
e is 65537 (0x010001)  
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.  
-----  
Common Name (eg: your user, host, or server name) [Easy-RSA CA]:openvpn-srv  
  
CA creation complete and you may now import and sign cert requests.  
Your new CA certificate file for publishing is at:  
/etc/openvpn/pki/ca.crt  
  
root@srv-slave:/etc/openvpn#
```

### 1.3 Certificats Serveur

🔧 Création du certificat et de la clé privé serveur :

```
serveur@srv-slave: ~  
CA creation complete and you may now import and sign cert requests.  
Your new CA certificate file for publishing is at:  
/etc/openvpn/pki/ca.crt  
  
root@srv-slave:/etc/openvpn# /usr/share/easy-rsa/easyrsa build-server-full serve  
r nopass  
Using SSL: openssl OpenSSL 1.1.1w 11 Sep 2023  
Generating a RSA private key  
.....+++++  
.....+++++  
writing new private key to '/etc/openvpn/pki/easy-rsa-3396.rhrfif/tmp.vgSGzt'  
-----  
Using configuration from /etc/openvpn/pki/easy-rsa-3396.rhrfif/tmp.k9hLP8  
Check that the request matches the signature  
Signature ok  
The Subject's Distinguished Name is as follows  
commonName :ASN.1 12:'server'  
Certificate is to be certified until Jul 30 00:02:03 2026 GMT (825 days)  
  
Write out database with 1 new entries  
Data Base Updated  
  
root@srv-slave:/etc/openvpn#
```

## Génération des paramètres Diffie Hellman dans /etc/openvpn/pki/dh.pem :

```
server@srv-slave: ~  
root@srv-slave:/etc/openvpn# /usr/share/easy-rsa/easyrsa gen-dh  
Using SSL: openssl OpenSSL 1.1.1w  11 Sep 2023  
Generating DH parameters, 2048 bit long safe prime, generator 2  
This is going to take a long time  
.....+.....+.....  
.....+......+......+......+  
.....+.....  
.....+......  
.....+......+.....  
.....  
.....+......+......  
.....+.+......  
.....+......+.....  
.....+......+......  
.....+......+.....  
.....+.+.+......  
.....+......  
.....+......+......  
.....+......+
```

## 1.4 Certificats Client

## Créer un certificat client1

```


root@srv-slave:/etc/openvpn# /usr/share/easy-rsa/easyrsa build-client-full client1 nopass
Using SSL: openssl OpenSSL 1.1.1w  11 Sep 2023
Generating a RSA private key
.....+++++
..+++++
writing new private key to '/etc/openvpn/pki/easy-rsa-3984.fSM92I/tmp.6bBvm8'
-----
Using configuration from /etc/openvpn/pki/easy-rsa-3984.fSM92I/tmp.aYlK0Q
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName                :ASN.1 12:'client1'
Certificate is to be certified until Jul 30 09:41:02 2026 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

root@srv-slave:/etc/openvpn#

```

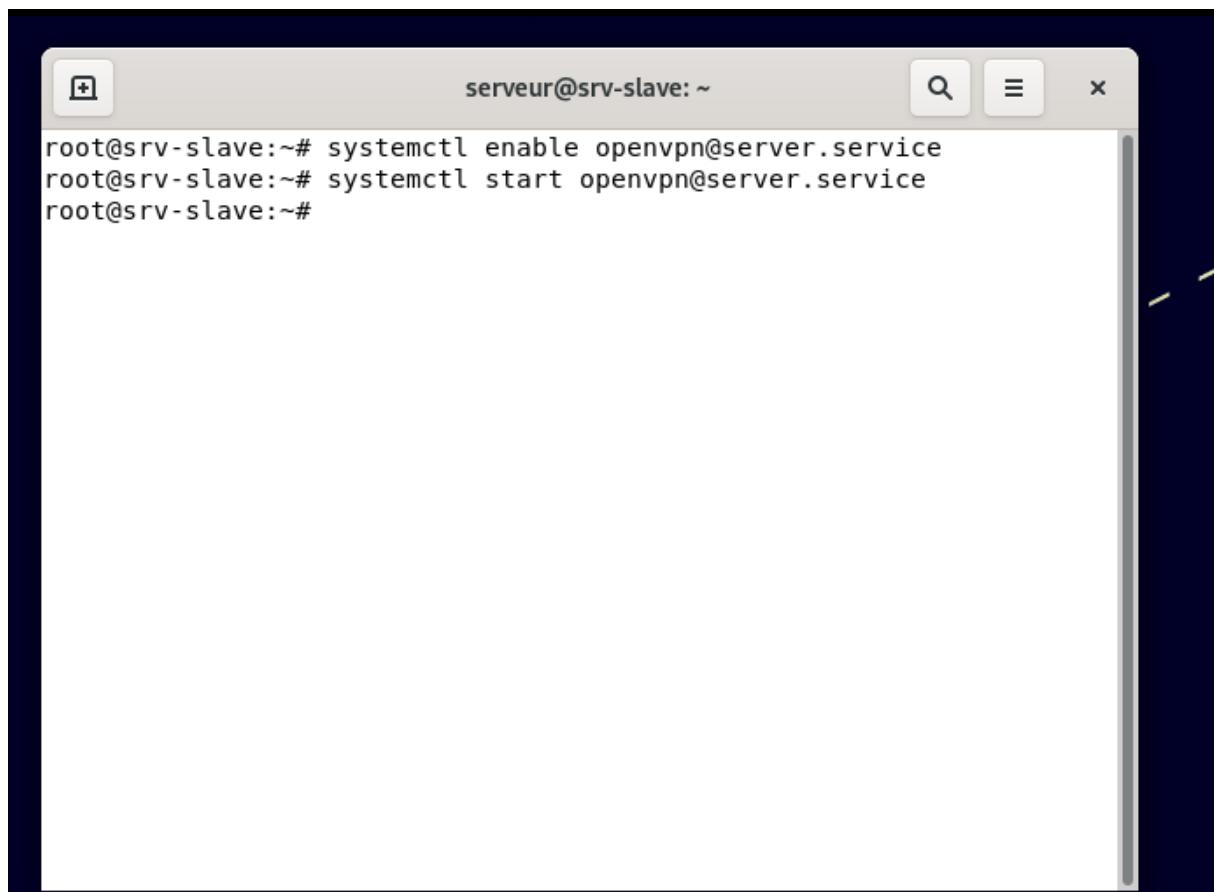
## 1.5 Fichier de configuration serveur



```
serveur@srv-slave: ~  
port 1194  
proto udp  
dev tun  
ca /etc/openvpn/pki/ca.crt  
cert /etc/openvpn/pki/issued/server.crt  
key /etc/openvpn/pki/private/server.key  
dh /etc/openvpn/pki/dh.pem  
server 10.50.8.0 255.255.255.0 # internal tun0 connection IP  
ifconfig-pool-persist ipp.txt  
keepalive 10 120  
comp-lzo # Compression - must be turned on at both end  
persist-key  
persist-tun  
push "dhcp-option DNS 192.168.0.111"  
push "dhcp-option DOMAIN exemple.com"  
push "route 192.168.0.0 255.255.255.0"  
status /var/log/openvpn-status.log  
verb 3 # verbose mode  
~  
~  
~  
~  
~  
-- INSERT --
```

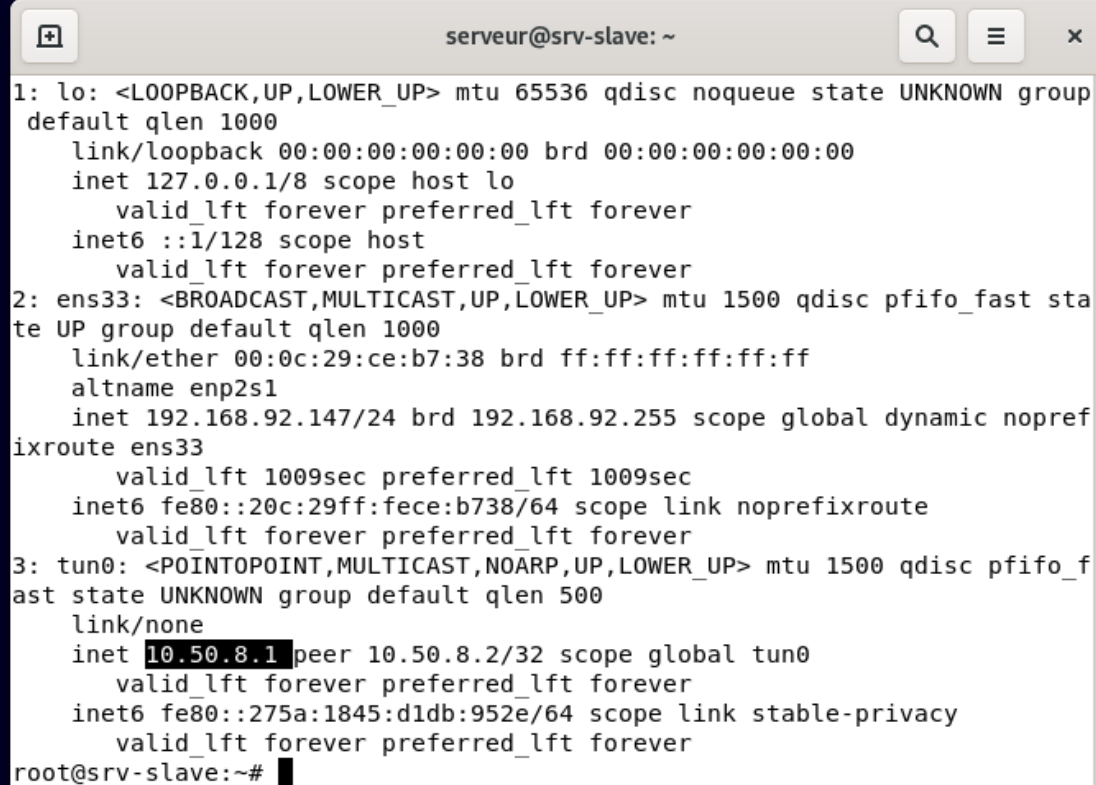
18,22 All

## 1.6 Démarrage du serveur



```
serveur@srv-slave: ~  
root@srv-slave:~# systemctl enable openvpn@server.service  
root@srv-slave:~# systemctl start openvpn@server.service  
root@srv-slave:~#
```

✚ Vérification :



```
serveur@srv-slave: ~  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group  
default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 00:0c:29:ce:b7:38 brd ff:ff:ff:ff:ff:ff  
    altname enp2s1  
    inet 192.168.92.147/24 brd 192.168.92.255 scope global dynamic nopref  
ixroute ens33  
        valid_lft 1009sec preferred_lft 1009sec  
    inet6 fe80::20c:29ff:fece:b738/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_f  
ast state UNKNOWN group default qlen 500  
    link/none  
    inet 10.50.8.1 peer 10.50.8.2/32 scope global tun0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::275a:1845:d1db:952e/64 scope link stable-privacy  
        valid_lft forever preferred_lft forever  
root@srv-slave:~#
```

## 1.7 Configuration mode routeur

✚ installer NfTables



```
serveur@srv-slave: ~  
root@srv-slave:~# sudo apt install nftables  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
nftables is already the newest version (0.9.8-3.1+deb11u2).  
0 upgraded, 0 newly installed, 0 to remove and 5 not upgraded.  
root@srv-slave:~#
```

### 🚦 Configurer les règles NAT

```
serveur@srv-slave: ~  
root@srv-slave:~# sudo nft add table ip NAT  
root@srv-slave:~# sudo nft add rule NAT my_masquerade ip saddr { 10.50.8.  
0/24 } oifname ens33 masquerade  
root@srv-slave:~# sudo nft add rule NAT my_masquerade ip saddr { 10.50.8.  
0/24 } oifname ens33 masquerade  
root@srv-slave:~# sudo systemctl enable nftables.service  
Created symlink /etc/systemd/system/sysinit.target.wants/nftables.service  
→ /lib/systemd/system/nftables.service.  
root@srv-slave:~# █
```

🚦 Activer le mode routeur:



A terminal window titled "serveur@srv-slave: ~" with search, menu, and close buttons. The terminal shows the command "sudo sysctl -p /etc/sysctl.conf" being executed. The prompt changes from "root@srv-slave:~#" to "root@srv-slave:~#" after the command is run. A yellow arrow points to the right side of the terminal window.

```
serveur@srv-slave: ~
root@srv-slave:~# sudo sysctl -p /etc/sysctl.conf
root@srv-slave:~#
```

```
serveur@srv-slave: ~  
#net.ipv4.conf.all.rp_filter=1  
  
# Uncomment the next line to enable TCP/IP SYN cookies  
# See http://lwn.net/Articles/277146/  
# Note: This may impact IPv6 TCP sessions too  
#net.ipv4.tcp_syncookies=1  
  
# Uncomment the next line to enable packet forwarding for IPv4  
net.ipv4.ip_forward=1  
  
# Uncomment the next line to enable packet forwarding for IPv6  
# Enabling this option disables Stateless Address Autoconfiguration  
# based on Router Advertisements for this host  
#net.ipv6.conf.all.forwarding=1  
  
#####  
# Additional settings - these settings can improve the network  
# security of the host and prevent against some network attacks  
# including spoofing attacks and man in the middle attacks through  
# redirection. Some network environments, however, require that these  
# settings are disabled so review and enable them as needed.  
#  
-- INSERT --
```

```
serveur@srv-slave: ~  
root@srv-slave:/home/serveur# sudo sysctl -p  
net.ipv4.ip_forward = 1  
root@srv-slave:/home/serveur#
```

## 2. Configuration du client

## 🔧 Installation de openvpn

```
client@debian: ~  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following additional packages will be installed:  
  easy-rsa libccid libpkcs11-helper1 opensc opensc-pkcs11 pcscd  
Suggested packages:  
  pcmciautils resolvconf openvpn-systemd-resolved  
The following NEW packages will be installed:  
  easy-rsa libccid libpkcs11-helper1 opensc opensc-pkcs11 openvpn pcscd  
0 upgraded, 7 newly installed, 0 to remove and 11 not upgraded.  
Need to get 2,374 kB of archives.  
After this operation, 7,227 kB of additional disk space will be used.  
Do you want to continue? [Y/n]  
Get:1 http://deb.debian.org/debian bullseye/main amd64 libccid amd64 1.4.34-1 [337 kB]  
Get:2 http://deb.debian.org/debian bullseye/main amd64 pcscd amd64 1.9.1-1 [98.1 kB]  
Get:3 http://deb.debian.org/debian bullseye/main amd64 easy-rsa all 3.0.8-1 [45.2 kB]  
Get:4 http://deb.debian.org/debian bullseye/main amd64 libpkcs11-helper1 amd64 1.27-1 [47.5 kB]  
Get:5 http://deb.debian.org/debian bullseye/main amd64 opensc-pkcs11 amd64 0.21.0-1 [880 kB]  
52% [5 opensc-pkcs11 688 kB/880 kB 78%] 68.9 kB/s 16s
```

## 🔧 Transfert des fichiers de certificats et clés

J'ai un problème lorsque j'essaie de transférer les fichiers nécessaires du serveur au client : un message 'Permission denied' s'affiche malgré la saisie du mot de passe correct, et les fichiers ne se transfèrent pas

```
serveur@srv-slave: ~  
root@srv-slave:~# scp user@192.168.92.143:/etc/openvpn/pki/issued/client1.crt /etc/openvpn/client1.crt  
user@192.168.92.143's password:  
Permission denied, please try again.  
user@192.168.92.143's password:  
Permission denied, please try again.  
user@192.168.92.143's password: █
```

#### 🔧 Création du fichier de configuration du client

```
client@debian: ~  
client  
dev tun  
proto udp  
remote 192.168.92.147 1194  
resolv-retry infinite  
nobind  
persist-key  
persist-tun  
ca ca.crt  
cert client1.crt  
key client1.key  
comp-lzo  
verb 3  
  
~  
~  
~  
~  
-- INSERT --  
4,22 All
```