

Mini projet :
Mise en œuvre d'un VPN avec Open VPN sous Linux

Elaboré par : **MERYEM ESSAFI**

Encadré par : **Mr. BOUKHDIR**

Année universitaire : 2021/2022



OBJECTIF DU PROJET :

L'objectif de ce mini-projet est de mettre en œuvre un Virtual Private Network (VPN) avec open VPN sous Linux



REMERCIEMENT

Nous remercions Mr Boukhdir, enseignant, de par sa disponibilité à répondre à toutes les questions liées à la réalisation de ce mini-projet.

Et Au terme de ce projet, nous tenons à témoigner notre profonde reconnaissance à notre cher professeur pour son encadrement et son encouragement, ses précieux conseils, et pour l'intérêt qu'il a porté pour ce travail ainsi que de nous avoir donner l'opportunité d'avoir une expérience en domaine de sécurité informatique, qui est un domaine vaste et très intéressant.

Ce genre de travaux est indispensable car ils peuvent nous servir dans plusieurs situations. Grâce à vous, on est désormais capable de manipuler l'outil **Open VPN**.



SOMMAIRE

Introduction	5
Sécurité informatique.....	5
Définition de VPN	6
Présentation de logiciel Open VPN.....	7
Mise en place d'un VPN compressé et non-crypté.....	8
Mise en place d'un VPN compressé et crypté.....	14
Effectuer les tests nécessaires pour vérifier le bon fonctionnement du VPN ...	20
Conclusion	34
Bibliographie	35



INTRODUCTION

La sécurité informatique consiste à protéger un système informatique contre toute violation, intrusion, dégradation ou vol de données au sein du système d'information.

Avec **l'essor d'internet**, et l'utilisation par la majorité des entreprises et des organisations de **processus informatisés**, les **menaces** visant les systèmes d'informations **n'ont cessés d'augmenter** et de **se sophistiquer**, faisant aujourd'hui de la sécurité informatique une **nécessité pour tous les types de structure**.





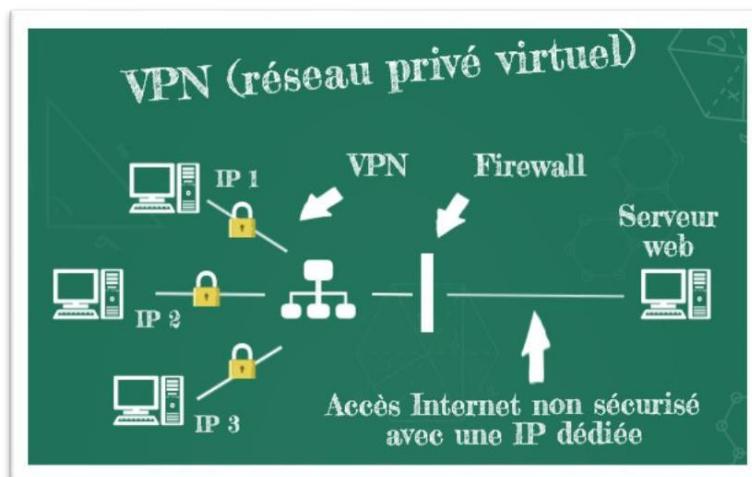
Définition de VPN

Un réseau privé virtuel (**Virtual Private Network**) est un tunnel sécurisé à l'intérieur d'un réseau (Internet notamment). Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente de celle de votre ordinateur.

Ce système est pratique pour surfer sur Internet avec une localisation différente de la vôtre. Un autre intérêt est le faible coût de l'accès Internet, à partir de 2,75 euros par mois pour les services les plus courants.

Le VPN est parfaitement légal : de nombreuses entreprises y ont recours pour protéger les échanges d'informations entre deux filiales à l'étranger par exemple.

→ Le VPN permet de surfer sur le web de manière **anonyme** et de choisir la géolocalisation de son adresse IP.





Présentation de logiciel Open VPN

OpenVPN est une solution logicielle libre complète permettant de créer différentes configurations de VPN (Virtual Private Network) ou réseaux privés virtuels pour accéder à des ordinateurs distants, créer un tunnel sécurisé de site à site, sécuriser une connexion Wifi, etc.

Avec OpenVPN, vous allez pouvoir enfermer votre sous-réseau dans un tunnel, protéger un réseau avec de l'OpenSSL ou encore accéder à distance à un ordinateur. OpenVPN vous permet d'accéder à un réseau local distant de manière sécurisée afin de pouvoir consulter des fichiers hébergés sur des ordinateurs distants.

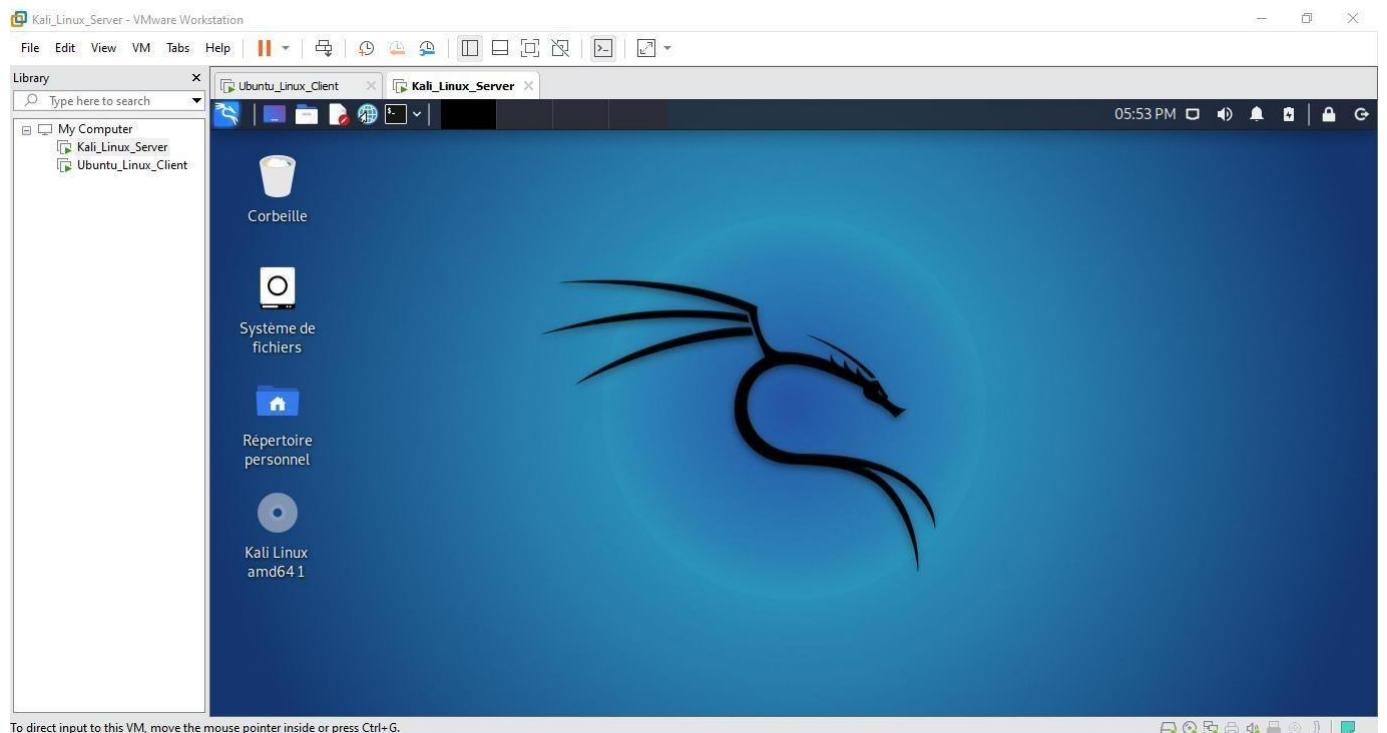
Mise en place d'un VPN compressé et non-crypté

On démarre la machine virtuelle **VMware Workstation**, après l'installation de deux versions de Linux sous cette machine virtuelle : **Kali Linux et Ubuntu Linux**.

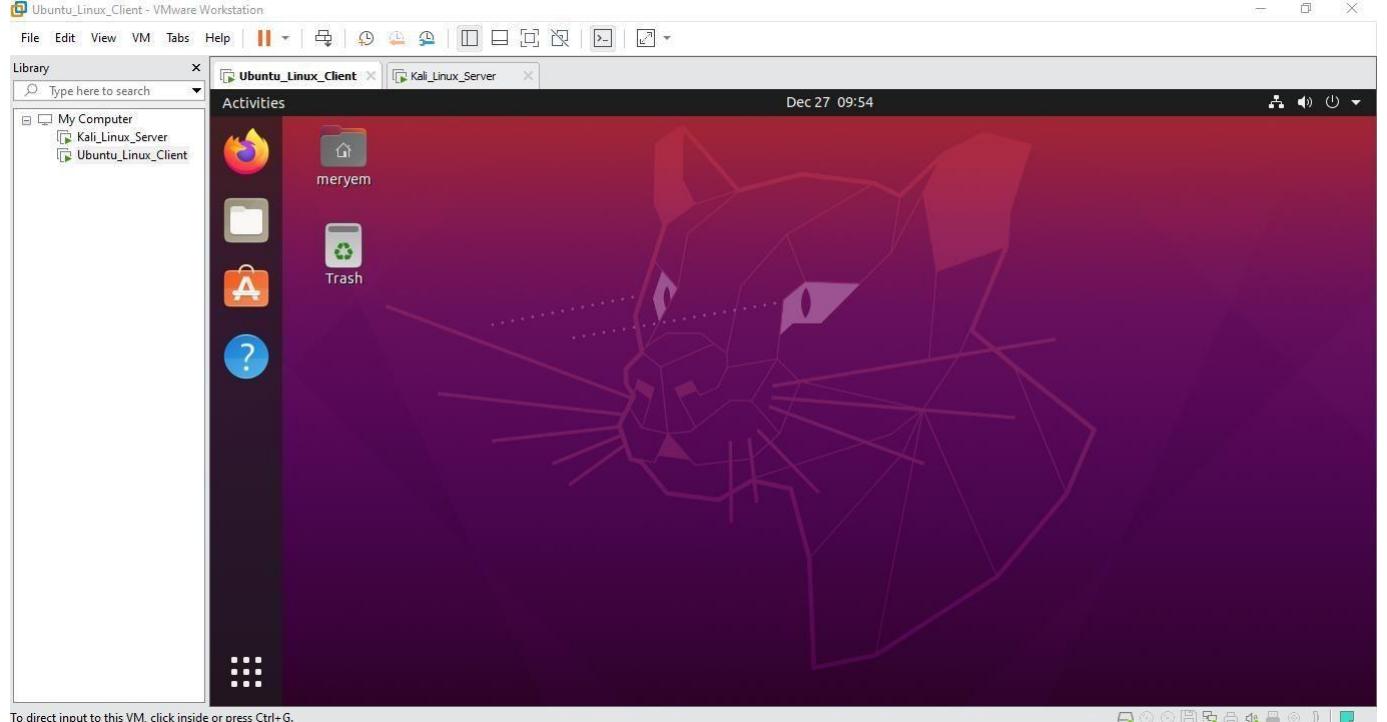
Le client : Ubuntu

Le serveur : Kali

Puis on lance les deux systèmes d'exploitation.



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



On fait la configuration nécessaire et on vérifier la connectivité.



Pour tester la connectivité réseau, il existe la commande **ping**.

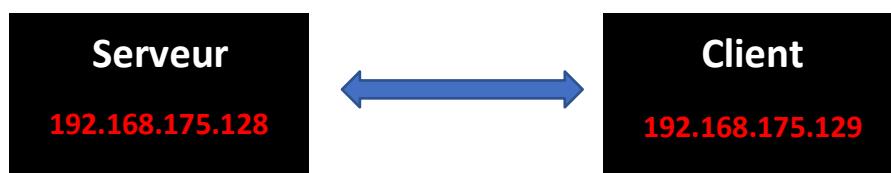
- Pour la machine serveur Kali, on tape la commande **ping** suivi par l'adresse IP de la machine client : **192.168.175.129**.

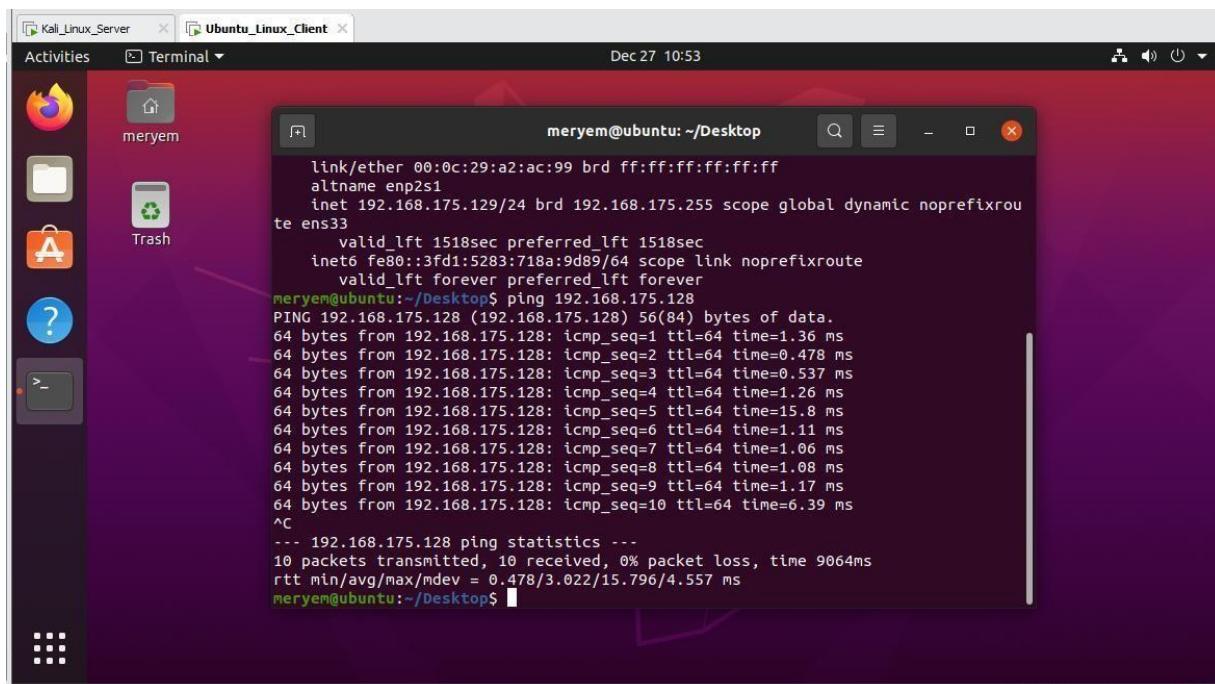
```
meryem@kali: ~
inet 192.168.175.128/24 brd 192.168.175.255 scope global dynamic noprefixroute eth0
    valid_lft 1751sec preferred_lft 1751sec
inet6 fe80::20c:29ff:fe25:1cb5/64 scope link noprefixroute
    valid_lft forever preferred_lft forever

(meryem㉿kali)-[~]
$ ping 192.168.175.129
PING 192.168.175.129 (192.168.175.129) 56(84) bytes of data.
64 bytes from 192.168.175.129: icmp_seq=1 ttl=64 time=0.746 ms
64 bytes from 192.168.175.129: icmp_seq=2 ttl=64 time=0.971 ms
64 bytes from 192.168.175.129: icmp_seq=3 ttl=64 time=0.992 ms
64 bytes from 192.168.175.129: icmp_seq=4 ttl=64 time=0.991 ms
64 bytes from 192.168.175.129: icmp_seq=5 ttl=64 time=1.03 ms
64 bytes from 192.168.175.129: icmp_seq=6 ttl=64 time=1.05 ms
64 bytes from 192.168.175.129: icmp_seq=7 ttl=64 time=1.01 ms
64 bytes from 192.168.175.129: icmp_seq=8 ttl=64 time=1.06 ms
64 bytes from 192.168.175.129: icmp_seq=9 ttl=64 time=1.03 ms
64 bytes from 192.168.175.129: icmp_seq=10 ttl=64 time=2.29 ms
64 bytes from 192.168.175.129: icmp_seq=11 ttl=64 time=1.02 ms
64 bytes from 192.168.175.129: icmp_seq=12 ttl=64 time=0.997 ms
64 bytes from 192.168.175.129: icmp_seq=13 ttl=64 time=1.08 ms
64 bytes from 192.168.175.129: icmp_seq=14 ttl=64 time=1.05 ms
64 bytes from 192.168.175.129: icmp_seq=15 ttl=64 time=1.02 ms
64 bytes from 192.168.175.129: icmp_seq=16 ttl=64 time=1.27 ms
64 bytes from 192.168.175.129: icmp_seq=17 ttl=64 time=1.10 ms
^C
--- 192.168.175.129 ping statistics ---
17 packets transmitted, 17 received, 0% packet loss, time 16049ms
rtt min/avg/max/mdev = 0.746/1.099/2.290/0.312 ms

(meryem㉿kali)-[~]
$
```

- Pour la machine Client Ubuntu, on tape la commande **ping** suivi par l'adresse IP de la machine Serveur : **192.168.175.128**.





```
(meryem㉿kali)-[~]
$ hostname -I
192.168.175.128

(meryem㉿kali)-[~]
$ sudo apt install openvpn
[sudo] Mot de passe de meryem :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openvpn est déjà la version la plus récente (2.5.1-3).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  python3-editor python3-ipython-genutils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 256 non mis à jour.

(meryem㉿kali)-[~]
$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2
2021-12-27 21:47:21 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2021-12-27 21:47:21 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [AEAD] built on May 14 2021
2021-12-27 21:47:21 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-27 21:47:21 ***** WARNING *****: All encryption and authentication features disabled -- All data will be tunneled as clear text and will not be protected against man-in-the-middle changes. PLEASE DO RECONSIDER THIS CONFIGURATION!
2021-12-27 21:47:22 TUN/TAP device tun1 opened
2021-12-27 21:47:22 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 21:47:22 net_iface_up: set tun1 up
2021-12-27 21:47:22 net_addr_pptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 21:47:22 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 21:47:22 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 21:47:22 UDPv4 link remote: [AF_UNSPEC]
```

Pour avoir ces adresses IP, il suffit de taper la commande **hostname -I**.

Ensuite on essaye d'installer OpenVPN sur les deux machines.



```

meryem@ubuntu: ~/Desktop
meryem@ubuntu:~$ hostname -I
192.168.175.129
meryem@ubuntu:~$ sudo apt install openvpn
[sudo] password for meryem:
Reading package lists... Done
Building dependency tree
Reading state information... Done
openvpn is already the newest version (2.4.7-1ubuntu2.20.04.3).
openvpn set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 144 not upgraded.
meryem@ubuntu:~$ sudo openvpn --dev tun1 --remote 192.168.175.128 --ifconfig 10.0.0.2 10.0.0.1
Mon Dec 27 13:52:49 2021 disabling NCP mode (--ncp-disable) because not in P2MP client or server mode
Mon Dec 27 13:52:49 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on Jul 19 2021
Mon Dec 27 13:52:49 2021 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.10
Mon Dec 27 13:52:49 2021 ***** WARNING *****: All encryption and authentication features disabled -- All data will be tunneled as clear text and will not be protected against man-in-the-middle changes. PLEASE DO RECONSIDER THIS CONFIGURATION!
Mon Dec 27 13:52:49 2021 TUN/TAP device tun1 opened
Mon Dec 27 13:52:49 2021 /sbin/ip link set dev tun1 up mtu 1500
Mon Dec 27 13:52:49 2021 /sbin/ip addr add dev tun1 local 10.0.0.2 peer 10.0.0.1
Mon Dec 27 13:52:49 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 13:52:49 2021 UDP link local (bound): [AF_INET][undef]:1194
Mon Dec 27 13:52:49 2021 UDP link remote: [AF_INET]192.168.175.128:1194
Mon Dec 27 13:52:49 2021 Peer Connection Initiated with [AF_INET]192.168.175.128:1194
Mon Dec 27 13:53:00 2021 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Mon Dec 27 13:53:00 2021 Initialization Sequence Completed

```

On va lancer le tunnel **tun1** à partir de la machine serveur.

```

meryem@kali: ~
meryem@kali:~$ 192.168.175.128
meryem@kali:~$ sudo apt install openvpn
[sudo] Mot de passe pour meryem :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openvpn est déjà la version la plus récente (2.5.1-3).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  python3-editor python3-ipython-genutils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 256 non mis à jour.

meryem@kali:~$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2
2021-12-27 21:47:21 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2021-12-27 21:47:21 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-27 21:47:21 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-27 21:47:21 ***** WARNING *****: All encryption and authentication features disabled -- All data will be tunneled as clear text and will not be protected against man-in-the-middle changes. PLEASE DO RECONSIDER THIS CONFIGURATION!
2021-12-27 21:47:22 TUN/TAP device tun1 opened
2021-12-27 21:47:22 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 21:47:22 net_iface_up: set tun1 up
2021-12-27 21:47:22 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 21:47:22 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 21:47:22 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 21:47:22 UDPv4 link remote: [AF_UNSPEC]
2021-12-27 21:52:48 Peer Connection Initiated with [AF_INET]192.168.175.129:1194
2021-12-27 21:52:49 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2021-12-27 21:52:49 Initialization Sequence Completed

```

- ➔ Donc le tunnel est ouvert avec le port par défaut **1194**.
- ➔ Le Serveur en écoute.
- ➔ On fera de même pour la machine Client (en ajoutant l'adresse de la machine Serveur).



Kali_Linux_Server x Ubuntu_Linux_Client x

meryem@kali: ~ 10:12 PM

Fichier Actions Éditer Vue Aide

```
192.168.175.128
(meryem@kali)-[~]
$ sudo apt install openvpn
[sudo] Mot de passe de meryem :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openvpn est déjà la version la plus récente (2.5.1-3).
Les paquets suivants ont été installés automatiquement et ne sont plus
python3-editor python3-ipython-genutils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 256 non mis à j

(meryem@kali)-[~]
$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2
2021-12-27 21:47:21 Cipher negotiation is disabled since neither P2MP
2021-12-27 21:47:21 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)]
2021-12-27 21:47:21 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO
2021-12-27 21:47:21 ***** WARNING *****: All encryption and authen
nd will not be protected against man-in-the-middle changes. PLEASE DO
2021-12-27 21:47:21 TUN/TAP device tun1 opened
2021-12-27 21:47:22 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 21:47:22 net_iface_up: set tun1 up
2021-12-27 21:47:22 net_addr_ptp_v4_addr: 10.0.0.1 peer 10.0.0.2 dev tu
2021-12-27 21:47:22 Could not determine IPv4/IPv6 protocol. Using AF_I
2021-12-27 21:47:22 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 21:47:22 UDPv4 link remote: [AF_UNSPEC]
2021-12-27 21:52:48 Peer Connection Initiated with [AF_INET]192.168.17
2021-12-27 21:52:49 WARNING: this configuration may cache passwords in
2021-12-27 21:52:49 Initialization Sequence Completed
[~]
```

Kali_Linux_Server x Ubuntu_Linux_Client x

Activities Terminal ▾ Dec 27 14:14

meryem@ubuntu: ~/Desktop

```
) because not in P2MP client or server mode
Mon Dec 27 13:52:49 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu
[SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AESD] built on Jul 19 2021
Mon Dec 27 13:52:49 2021 library versions: OpenSSL 1.1.1f
31 Mar 2020, LZO 2.10
Mon Dec 27 13:52:49 2021 ***** WARNING *****: All encr
yption and authentication features disabled -- All data wi
ll be tunnelled as clear text and will not be protected ag
ainst man-in-the-middle changes. PLEASE DO RECONSIDER THIS
CONFIGURATION!
Mon Dec 27 13:52:49 2021 TUN/TAP device tun1 opened
Mon Dec 27 13:52:49 2021 /sbin/ip link set dev tun1 up mtu
1500
Mon Dec 27 13:52:49 2021 /sbin/ip addr add dev tun1 local
10.0.0.2 peer 10.0.0.1
Mon Dec 27 13:52:49 2021 TCP/UDP: Preserving recently used
remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 13:52:49 2021 UDP link local (bound): [AF_INET]
[undef]:1194
Mon Dec 27 13:52:49 2021 UDP link remote: [AF_INET]192.168
.175.128:1194
Mon Dec 27 13:52:59 2021 Peer Connection Initiated with [A
F_INET]192.168.175.128:1194
Mon Dec 27 13:53:00 2021 WARNING: this configuration may c
ache passwords in memory -- use the auth-nocache option to
prevent this
Mon Dec 27 13:53:00 2021 Initialization Sequence Completed
[~]
```

meryem@ubuntu: ~

```
meryem@ubuntu:~$ hostname -I
192.168.175.129 10.0.0.2
meryem@ubuntu:~$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=2.66 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=2.20 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=2.05 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=2.26 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=1.92 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=2.09 ms
^C
--- 10.0.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5010ms
rtt min/avg/max/mdev = 1.916/2.195/2.662/0.235 ms
meryem@ubuntu:~$
```



Kali_Linux_Server X Ubuntu_Linux_Client X

meryem@kali: ~ 10:19 PM

Fichier Actions Éditer Vue Aide

```
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openvpn est déjà la version la plus récente (2.5.1-3).
Les paquets suivants ont été installés automatiquement et ne sont plus
    python3-editor python3-ipython-genutils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 256 non mis à j

(meryem@kali)~] $ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2
2021-12-27 21:47:21 Cipher negotiation is disabled since neither P2MP
2021-12-27 21:47:21 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)]
2021-12-27 21:47:21 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO
2021-12-27 21:47:21 ***** WARNING *****: All encryption and authen
nd will not be protected against man-in-the-middle changes. PLEASE DO
2021-12-27 21:47:22 TUN/TAP device tun1 opened
2021-12-27 21:47:22 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 21:47:22 net_iface_up: set tun1 up
2021-12-27 21:47:22 net_addrptp_v4_add: 10.0.0.1 dev tun1
2021-12-27 21:47:22 Could not determine IPv4/IPv6 protocol. Using AF_I
2021-12-27 21:47:22 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 21:47:22 UDPv4 link remote: [AF_UNSPEC]
2021-12-27 21:52:48 Peer Connection Initiated with [AF_INET]192.168.17
2021-12-27 21:52:49 WARNING: this configuration may cache passwords in
2021-12-27 21:52:49 Initialization Sequence Completed
2021-12-27 22:19:11 event_wait : Interrupted system call (code=4)
2021-12-27 22:19:11 net_addrptp_v4_del: 10.0.0.1 dev tun1
2021-12-27 22:19:11 SIGTERM[hard,] received, process exiting

(meryem@kali)~] $
```

Kali_Linux_Server X Ubuntu_Linux_Client X

Activities Terminal Dec 27 14:21

meryem@ubuntu: ~/Desktop

```
Mon Dec 27 13:52:49 2021 ***** WARNING *****: All encr
ption and authentication features disabled -- All data wi
ll be tunneled as clear text and will not be protected ag
ainst man-in-the-middle changes. PLEASE DO RECONSIDER THIS
CONFIGURATION!
Mon Dec 27 13:52:49 2021 TUN/TAP device tun1 opened
Mon Dec 27 13:52:49 2021 /sbin/ip link set dev tun1 up mtu
1500
Mon Dec 27 13:52:49 2021 /sbin/ip addr add dev tun1 local
10.0.0.2 peer 10.0.0.1
Mon Dec 27 13:52:49 2021 TCP/UDP: Preserving recently used
remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 13:52:49 2021 UDP link local (bound): [AF_INET]
[undef]:1194
Mon Dec 27 13:52:49 2021 UDP link remote: [AF_INET]192.168
.175.128:1194
Mon Dec 27 13:52:59 2021 Peer Connection Initiated with [A
F_INET]192.168.175.128:1194
Mon Dec 27 13:53:00 2021 WARNING: this configuration may c
ache passwords in memory -- use the auth-nocache option to
prevent this
Mon Dec 27 13:53:00 2021 Initialization Sequence Completed
Mon Dec 27 14:20:52 2021 event_wait : Interrupted system c
all (code=4)
Mon Dec 27 14:20:52 2021 /sbin/ip addr del dev tun1 local
10.0.0.2 peer 10.0.0.1
Mon Dec 27 14:20:52 2021 SIGTERM[hard,] received, process
exiting
meryem@ubuntu:~/Desktop$
```

meryem@ubuntu: ~ 192.168.175.129 10.0.0.2

PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.

64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.056 ms

64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.070 ms

64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.068 ms

64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.068 ms

64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.079 ms

^C

--- 10.0.0.2 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 41
04ms

rtt min/avg/max/mdev = 0.056/0.068/0.079/0.007 ms

meryem@ubuntu: ~\$ sudo killall openvpn

[sudo] password for meryem:

meryem@ubuntu: ~\$

mouse pointer inside or press Ctrl+G.

- ➔ Donc un tunnel virtuel est établi sans aucun problème (sans qu'il ça soit crypté).
- ➔ Pour passer a la deuxième partie on arrête le tunnel avec la commande **killall openvpn**.



Partie 2

Dans cette partie, on va lancer les mêmes commandes tout en s'appuyions sur une clé partagée entre les deux machines.

The screenshot shows a terminal window titled 'Kali_Linux_Server' and 'Ubuntu_Linux_Client'. The user 'meryem' is logged in on the Kali Linux server. The terminal displays the following commands and output:

```
meryem@kali: ~
Fichier Actions Éditer Vue Aide
(meryem@kali)-[~]
$ mkdir TP_openVPN
(meryem@kali)-[~]
$ cd TP_openVPN
(meryem@kali)-[~/TP_openVPN]
$ sudo openvpn --genkey --secret key
[sudo] Mot de passe de meryem :
2021-12-27 22:26:03 WARNING: Using --genkey --secret filename is DEPRECATED. Use --genkey secret filename instead.
(meryem@kali)-[~/TP_openVPN]
$ ls
key
(meryem@kali)-[~/TP_openVPN]
$ sudo cat key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
fc3b8983c51812740e217fc349e7767
455088012139f9ab4855a96462a06271
41b718bfe95c04d1c6755f0e62aa22c
a5504ea5b0bef62fc2e3b2dc4ca80ed
9d503083445e61bc0b63e896f0ad11b4
12f275cbc46278724172df5888925b1
0f84b4d23d44623033463a45d06903bb
59a2fdeeb70e287053afdc59fe18229
d1166dc68a96a9b90ac5acefad3e0ed
-----END OpenVPN Static key V1-----
```

A red box highlights the generated key content, specifically the long string of characters starting with 'fc3b8983c51812740e217fc349e7767'.

- ➔ On crée un répertoire : **TP_openVPN**, on y accède.
- ➔ Puis on va générer notre clé (clé de 2048 bit).



The screenshot shows a terminal window with two panes. The left pane displays the command output for generating an OpenVPN static key:

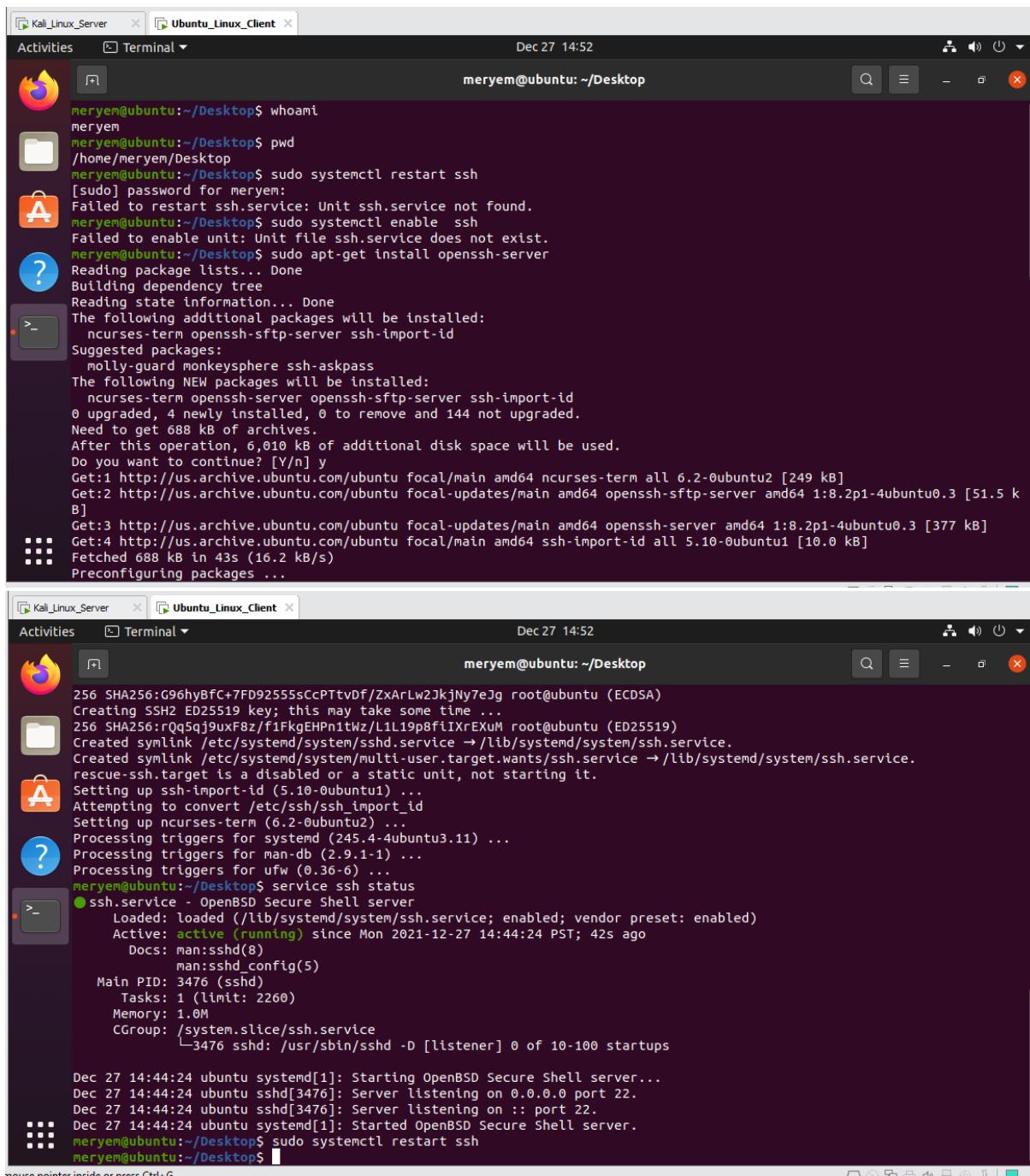
```
(meryem㉿kali)-[~/TP_openVPN]
$ ls
key
(meryem㉿kali)-[~/TP_openVPN]
$ sudo cat key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
fc3b8983c51812740e217fc349e7767
455088012139f9ab4855a96462a06271
41b7180fe965c04d1c6755f0e62a22c
a5504ea5b0bef62fc2e33b2dc4ca80ed
9d503083445e61bc0b63e896f0ad11b4
12f275cbc46278724172d4f5888925b1
0f84b4d23d44623033463aa5d06903bb
59a2fdeeb70e287053afdc59fe18229
d1166dc68a96a9b90ac5acefafd3e0ed
d6d6569a5053a3e36c17907a5d05fba
13a4dalec784c984a13c01ead0ea275
e2f4faa67f447fd9716d85c53e5c6089
ded63fad4771be5de4be7c4bd02f7d68
ad60033bdb939a56c2686dea126d91cb
aec114ff77b461925c0196db2e997f3
a8de0d7be9a2441532de89dc6f4f823f
-----END OpenVPN Static key V1-----
```

The right pane shows the command to use SCP:

```
(meryem㉿kali)-[~/TP_openVPN]
$ scp
```

Usage information for the SCP command is displayed:

```
usage: scp [-346ABCOpqRrsTv] [-c cipher] [-D sftp_server_path] [-F ssh_
```



```
meryem@ubuntu:~/Desktop$ whoami
meryem
meryem@ubuntu:~/Desktop$ pwd
/home/meryem/Desktop
meryem@ubuntu:~/Desktop$ sudo systemctl restart ssh
[sudo] password for meryem:
Failed to restart ssh.service: Unit ssh.service not found.
meryem@ubuntu:~/Desktop$ sudo systemctl enable ssh
Failed to enable unit: Unit file ssh.service does not exist.
meryem@ubuntu:~/Desktop$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-sftp-server ssh-import-id
Suggested packages:
  molly-guard monkeysphere ssh-askpass
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
0 upgraded, 4 newly installed, 0 to remove and 144 not upgraded.
Need to get 688 kB of archives.
After this operation, 6,010 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ncurses-term all 6.2-0ubuntu2 [249 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-sftp-server amd64 1:8.2p1-4ubuntu0.3 [51.5 kB]
Get:3 http://us.archive.ubuntu.com/ubuntu focal-updates/main amd64 openssh-server amd64 1:8.2p1-4ubuntu0.3 [377 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu focal/main amd64 ssh-import-id all 5.10-0ubuntu1 [10.0 kB]
Fetched 688 kB in 43s (16.2 kB/s)
Preconfiguring packages ...
meryem@ubuntu:~/Desktop$ 
256 SHA256:G96hyBfC+7FD92555sCcPTtvDf/ZxArLw2JkjNy7eJg root@ubuntu (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:rQq5qj9uxF8z/f1fkgeHPn1tWz/L1l19p8flXrExUM root@ubuntu (ED25519)
Created symlink /etc/systemd/system/sshd.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Setting up ssh-import-id (5.10-0ubuntu1) ...
Attempting to convert /etc/ssh/ssh_import_id
Setting up ncurses-term (6.2-0ubuntu2) ...
Processing triggers for systemd (245.4-4ubuntu3.11) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for ufw (0.36-6) ...
meryem@ubuntu:~/Desktop$ service ssh status
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2021-12-27 14:44:24 PST; 42s ago
    Docs: man:sshd(8)
           man:sshd_config(5)
  Main PID: 3476 (sshd)
     Tasks: 1 (limit: 2260)
   Memory: 1.0M
      CPU: 0.000 CPU(s) (idle)
     CGroup: /system.slice/ssh.service
             └─3476 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

Dec 27 14:44:24 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Dec 27 14:44:24 ubuntu sshd[3476]: Server listening on 0.0.0.0 port 22.
Dec 27 14:44:24 ubuntu sshd[3476]: Server listening on :: port 22.
Dec 27 14:44:24 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
meryem@ubuntu:~/Desktop$ sudo systemctl restart ssh
meryem@ubuntu:~/Desktop$ 
```



```

meryem@kali:~/TP_op...
meryem@kali:~/TP_op...
Clique pour atteindre l'espace de travail 3
Fichier Actions Éditer Vue Aide
lost connection
(meryem@kali)-[~/TP_openVPN]
$ scp key meryem@192.168.175.129:/home/meryem/Desktop      1 ✘
The authenticity of host '192.168.175.129 (192.168.175.129)' can't be established.
ED25519 key fingerprint is SHA256:rQq5qj9uxF8z/f1FkgEHFn1tWz/L1L19p8fiI
XrExUm.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.175.129' (ED25519) to the list of known hosts.
meryem@192.168.175.129's password:
key: Permission denied

(meryem@kali)-[~/TP_openVPN]
$ sudo scp key meryem@192.168.175.129:/home/meryem/Desktop      1 ✘
[sudo] Mot de passe de meryem :
The authenticity of host '192.168.175.129 (192.168.175.129)' can't be established.
ED25519 key fingerprint is SHA256:rQq5qj9uxF8z/f1FkgEHFn1tWz/L1L19p8fiIX
rExUm.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.175.129' (ED25519) to the list of known hosts.
meryem@192.168.175.129's password:
key          100%  636   55.9KB/s  00:00

(meryem@kali)-[~/TP_openVPN]
$ 

```

or press Ctrl+G.

```

Activities Terminal ▾ Dec 27 14:54
meryem@ubuntu: ~/Desktop
└ 3476 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
Dec 27 14:44:24 ubuntu systemd[1]: Starting OpenBSD Secure Shell server...
Dec 27 14:44:24 ubuntu sshd[3476]: Server listening on 0.0.0.0 port 22.
Dec 27 14:44:24 ubuntu sshd[3476]: Server listening on :: port 22.
Dec 27 14:44:24 ubuntu systemd[1]: Started OpenBSD Secure Shell server.
meryem@ubuntu:~/Desktop$ sudo systemctl restart ssh
meryem@ubuntu:~/Desktop$ cat key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
fc3b8983c51812740e217fc349e7767
455088012139f9ab4855a96462a06271
41b718bfe965c04d1c6755f0e62aa22c
a5504ea5b0bef62fc2e33b2dc4ca80ed
9d503083445e61bc0b63e896f0ad11b4
12f275cbc46278724172d4f5888925b1
0fb4b4d23d44623033463a45d06903bb
59a2fdeeb70e287053afca59fe18229
d1166dc68a96a9b90ac5acefafd3e0ed
d6d6569a5053a3e36c17907a5d05fbaa
13a4da1ee784c984a13c014ead0ea275
e2f4faa67f447fd9716d85c53e5c6b89
ded63fad4771be5de4be7c4bd02f7d68
ad60033db939a56c2686dea126d91cb
aec114ff77b461925c0196dbb2e997f3
a8de0d7be9a2441532de89dc6f4f823f
-----END OpenVPN Static key V1-----
meryem@ubuntu:~/Desktop$ 

```

➔ la clé est partagée avec la machine client avec succès.



Kali_Linux_Server X Ubuntu_Linux_Client X

meryem@kali: ~/TP_op...

11:00 PM

```
meryem@192.168.175.129's password:
key                                     100% 636   55.9KB/s  00:00

(meryem@kali) [~/TP_openVPN]
$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2 --secret key
2021-12-27 22:59:16 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2021-12-27 22:59:16 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-27 22:59:16 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-27 22:59:16 WARNING: INSECURE cipher (BF-CBC) with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 WARNING: INSECURE cipher (BF-CBC) with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 WARNING: INSECURE cipher (BF-CBC) with block size less than 128 bit (64 bit). This allows attacks like SWEET32. Mitigate by using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 TUN/TAP device tun1 opened
2021-12-27 22:59:16 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 22:59:16 net_iface_up: set tun1 up
2021-12-27 22:59:16 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 22:59:16 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 22:59:16 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 22:59:16 UDPv4 link remote: [AF_UNSPEC]
```

Kali_Linux_Server X Ubuntu_Linux_Client X

meryem@kali: ~/TP_op...

11:03 PM

```
y using a --cipher with a larger block size (e.g. AES-256-CBC). Support for these insecure ciphers will be removed in OpenVPN 2.6.
2021-12-27 22:59:16 TUN/TAP device tun1 opened
2021-12-27 22:59:16 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 22:59:16 net_iface_up: set tun1 up
2021-12-27 22:59:16 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 22:59:16 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 22:59:16 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 22:59:16 UDPv4 link remote: [AF_UNSPEC]
^C2021-12-27 23:01:22 event_wait : Interrupted system call (code=4)
2021-12-27 23:01:22 net_addr_ptp_v4_del: 10.0.0.1 dev tun1
2021-12-27 23:01:22 SIGINT[hard,] received, process exiting

(meryem@kali) [~/TP_openVPN]
$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2 --secret key --cipher AES-256-CBC
2021-12-27 23:03:25 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2021-12-27 23:03:25 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-27 23:03:25 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-27 23:03:25 TUN/TAP device tun1 opened
2021-12-27 23:03:25 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 23:03:25 net_iface_up: set tun1 up
2021-12-27 23:03:25 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 23:03:25 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 23:03:25 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 23:03:25 UDPv4 link remote: [AF_UNSPEC]
```



```
Kali_Linux_Server x Ubuntu_Linux_Client x
Activities Terminal ▾ Dec 27 15:21
meryem@ubuntu: ~
y --cipher AES-256-CBC
Mon Dec 27 15:13:30 2021 disabling NCP mode (--ncp-disable) because not in P2MP client or server mode
Mon Dec 27 15:13:30 2021 WARNING: cannot stat file '/home/Desktop/key': No such file or directory (errno=2)
Options error: --secret fails with '/home/Desktop/key': No such file or directory (errno=2)
Options error: Please correct these errors.
Use --help for more information.
meryem@ubuntu: $ sudo openvpn --dev tun1 --remote 192.168.175.128 --ifconfig 10.0.0.2 10.0.0.1 --secret home/meryem/Desktop/key --cipher AES-256-CBC
Mon Dec 27 15:15:03 2021 disabling NCP mode (--ncp-disable) because not in P2MP client or server mode
Mon Dec 27 15:15:03 2021 WARNING: cannot stat file '/home/meryem/Desktop/key': No such file or directory (errno=2)
Options error: --secret fails with '/home/meryem/Desktop/key': No such file or directory (errno=2)
Options error: Please correct these errors.
Use --help for more information.
meryem@ubuntu: $ sudo openvpn --dev tun1 --remote 192.168.175.128 --ifconfig 10.0.0.2 10.0.0.1 --secret /home/meryem/Desktop/key --cipher AES-256-CBC
Mon Dec 27 15:18:46 2021 disabling NCP mode (--ncp-disable) because not in P2MP client or server mode
Mon Dec 27 15:18:46 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AESNI] built on Jul 19 2021
Mon Dec 27 15:18:46 2021 library versions: OpenSSL 1.1.1f 31 Mar 2020, LZO 2.10
Mon Dec 27 15:18:46 2021 TUN/TAP device tun1 opened
Mon Dec 27 15:18:46 2021 /sbin/ip link set dev tun1 up mtu 1500
Mon Dec 27 15:18:46 2021 /sbin/ip addr add dev tun1 local 10.0.0.2 peer 10.0.0.1
Mon Dec 27 15:18:46 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 15:18:46 2021 UDP link local (bound): [AF_INET][undef]:1194
Mon Dec 27 15:18:46 2021 UDP link remote: [AF_INET]192.168.175.128:1194
Mon Dec 27 15:18:56 2021 Peer Connection Initiated with [AF_INET]192.168.175.128:1194
Mon Dec 27 15:18:57 2021 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
Mon Dec 27 15:18:57 2021 Initialization Sequence Completed
```

Kali_Linux_Server X [Ubuntu_Linux_Client X] meryem@kali: ~ 11:27 PM

Fichier Actions Éditer Vue Aide

```
2021-12-27 23:03:25 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 23:03:25 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 23:03:25 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 23:03:25 UDPv4 link remote: [AF_UNSPEC]
[2021-12-27 23:06:01 event_wait : interrupted system call (code=4)
2021-12-27 23:06:01 net_addr_ptp_v4_del: 10.0.0.1 dev tun1
2021-12-27 23:06:01 SIGINT[hard,] received, process exiting

(meryem@kali)-[~/TP_openVPN]
$ sudo openvpn --dev tun1 --ifconfig 10.0.0.1 10.0.0.2 --secret key --cipher AES-256-CBC
2021-12-27 23:06:11 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2021-12-27 23:06:11 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-27 23:06:11 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2 .10
2021-12-27 23:06:11 TUN/TAP device tun1 opened
2021-12-27 23:06:11 net_iface_mtu_set: mtu 1500 for tun1
2021-12-27 23:06:11 net_iface_up: set tun1 up
2021-12-27 23:06:11 net_addr_ptp_v4_add: 10.0.0.1 peer 10.0.0.2 dev tun1
2021-12-27 23:06:11 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-27 23:06:11 UDPv4 link local (bound): [AF_INET][undef]:1194
2021-12-27 23:06:11 UDPv4 link remote: [AF_UNSPEC]
2021-12-27 23:18:46 Peer Connection Initiated with [AF_INET]192.168.175.129:1194
2021-12-27 23:18:46 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2021-12-27 23:18:46 Initialization Sequence Completed
```

(meryem@kali)-[~]
\$ hostname -I
192.168.175.128 10.0.0.1

(meryem@kali)-[~]
\$ ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=1.07 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=1.95 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=2.05 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=1.95 ms
^C
--- 10.0.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.065/1.753/2.048/0.399 ms

(meryem@kali)-[~]
\$



Partie 3

Le but est de chiffrer la communication.

```

Kali_Linux_Server x Ubuntu_Linux_Client x
meryem@kali: ~
01:28 AM

Fichier Actions Éditer Vue Aide
Traitement des actions différées (« triggers ») pour man-db (2.9.4-2) ...
Traitement des actions différées (« triggers ») pour mailcap (3.70) ...
Traitement des actions différées (« triggers ») pour kali-menu (2021.4.2) ...
Traitement des actions différées (« triggers ») pour desktop-file-utils (0.26-1) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.31-13) ...

(meryem@kali)-[~]
$ sudo apt install openvpn easy-rsa
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
easy-rsa est déjà la version la plus récente (3.0.8-1).
openvpn est déjà la version la plus récente (2.5.1-3).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  python3-editor python3-ipython-genutils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 256 non mis à jour.

(meryem@kali)-[~]
$ sudo apt-get update
Récception de :1 http://kali.download/kali kali-rolling InRelease [30,6 kB]
Récception de :2 http://kali.download/kali kali-rolling/main amd64 Packages [17,9 MB]
Récception de :3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [39,9 MB]
Récception de :4 http://kali.download/kali kali-rolling/contrib amd64 Packages [114 kB]
Récception de :5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [153 kB]
Récception de :6 http://kali.download/kali kali-rolling/non-free amd64 Packages [210 kB]
Récception de :7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [964 kB]
59,3 Mo réceptionnés en 16s (3 804 ko/s)
Lecture des listes de paquets... Fait

(meryem@kali)-[~]
$ 

```

→ On installe **OpenVPN easy-rsa**, ensuite on le met à jour avec la commande `apt-get update` et on relance l'installation.

```

Kali_Linux_Server x Ubuntu_Linux_Client x
root@kali:/etc/openvpn/easy-rsa
01:46 AM

Fichier Actions Éditer Vue Aide
(meryem@kali)-[~]
$ ls /etc/openvpn/
server.txt serveur.txt

(meryem@kali)-[~]
$ sudo make-cadir /etc/openvpn/easy-rsa
[sudo] Mot de passe de meryem :

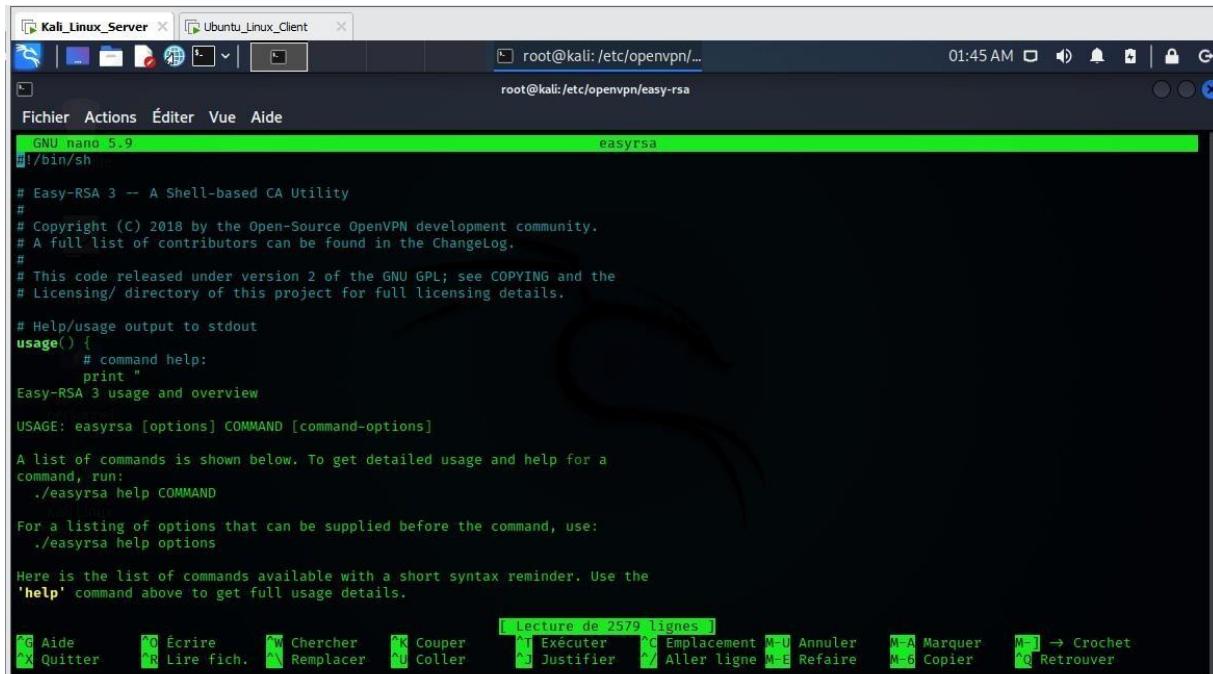
(meryem@kali)-[~]
$ ls /etc/openvpn/
easy-rsa server.txt serveur.txt

(meryem@kali)-[~]
$ cd /etc/openvpn/
(meryem@kali)-[/etc/openvpn]
$ sudo su
(root@kali)-[/etc/openvpn]
# cd easy-rsa/
(root@kali)-[/etc/openvpn/easy-rsa]
# ls
easyrsa openssl-easyrsa.cnf vars x509-types
(root@kali)-[/etc/openvpn/easy-rsa]
# nano easyrsa
(root@kali)-[/etc/openvpn/easy-rsa]
# 

```



→ On copie easy-rsa dans le répertoire openvpn.



```

root@kali:/etc/openvpn/easy-rsa
GNU nano 5.9                         easyrsa
#!/bin/sh

# Easy-RSA 3 -- A Shell-based CA Utility
#
# Copyright (C) 2018 by the Open-Source OpenVPN development community.
# A full list of contributors can be found in the ChangeLog.
#
# This code released under version 2 of the GNU GPL; see COPYING and the
# Licensing/ directory of this project for full licensing details.

# Help/usage output to stdout
usage() {
    # command help:
    print "
Easy-RSA 3 usage and overview

USAGE: easyrsa [options] COMMAND [command-options]

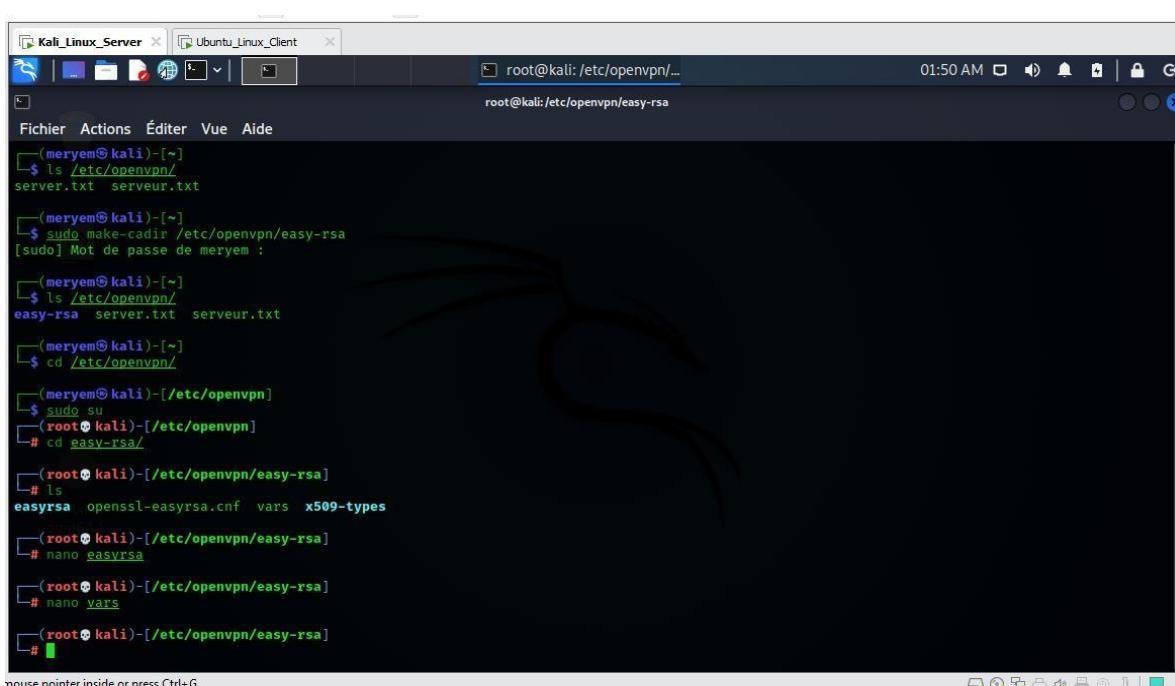
A list of commands is shown below. To get detailed usage and help for a
command, run:
./easyrsa help COMMAND

For a listing of options that can be supplied before the command, use:
./easyrsa help options

Here is the list of commands available with a short syntax reminder. Use the
'help' command above to get full usage details.

[ Lecteur de 2579 lignes ]
  Aide      Écrire      Chercher      Couper      Exécuter      Emplacement      Annuler      Marquer      → Crochet
  Quitter   Lire fich.  Remplacer   Collier      Justifier     Aller ligne      Réfaire      Copier      Retrouver

```



```

root@kali:/etc/openvpn/easy-rsa
ls /etc/openvpn/
server.txt  serveur.txt

ls /etc/openvpn/
easy-rsa  server.txt  serveur.txt

cd /etc/openvpn/
ls
easyrsa  openssl-easyrsa.cnf  vars  x509-types

nano easyrsa
nano vars

[ root@kali /etc/openvpn/easy-rsa ]
# ls
easyrsa  openssl-easyrsa.cnf  vars  x509-types
# nano easyrsa
# nano vars
# 

```



Kali_Linux_Server X Ubuntu_Linux_Client X

root@kali:/etc/openvpn/... 01:50 AM

```
Fichier Actions Éditer Vue Aide
GNU nano 5.9 vars
# Easy-RSA 3 parameter settings

# NOTE: If you installed Easy-RSA from your distro's package manager, don't edit
# this file in place -- instead, you should copy the entire easy-rsa directory
# to another location so future upgrades don't wipe out your changes.

# HOW TO USE THIS FILE
#
# vars.example contains built-in examples to Easy-RSA settings. You MUST name
# this file 'vars' if you want it to be used as a configuration file. If you do
# not, it WILL NOT be automatically read when you call easyrsa commands.
#
# It is not necessary to use this config file unless you wish to change
# operational defaults. These defaults should be fine for many uses without the
# need to copy and edit the 'vars' file.
#
# All of the editable settings are shown commented and start with the command
# 'set_var' -- this means any set_var command that is uncommented has been
# modified by the user. If you're happy with a default, there is no need to
# define the value to its default.

# NOTES FOR WINDOWS USERS
#
# Paths for Windows *MUST* use forward slashes, or optionally double-escaped
# backslashes (single forward slashes are recommended.) This means your path to
# the openssl binary might look like this:
# "C:/Program Files/OpenSSL-Win32/bin/openssl.exe"

[ Lecture de 221 lignes ]
Aide Écrire Chercher Couper Exécuter Emplacement Annuler Marquer → Crochet
Quitter Lire fich. Remplacer Coller Justifier Aller ligne Retrouver Copier Retrouver
```

Kali_Linux_Server X Ubuntu_Linux_Client X

root@kali:/etc/openvpn/... 02:02 AM

```
Fichier Actions Éditer Vue Aide

[root@kali ~]# ./easysrsa build-ca
Using SSL: openssl OpenSSL 1.1.1l 24 Aug 2021

Enter New CA Key Passphrase:
Re-Enter New CA Key Passphrase:
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x10001)
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]:
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/etc/openvpn/easy-rsa/pki/ca.crt

[root@kali ~]# ls
easysrsa openssl-easysrsa.cnf pki vars x509-types

[root@kali ~]#
```





```
Kali_Linux_Server | Ubuntu_Linux_Client
root@kali: /etc/openvpn/...
root@kali: /etc/openvpn/easy-rsa
Fichier Actions Éditer Vue Aide
Capture d'écran prise
Voir l'image
DH parameters of size 2048 created at /etc/openvpn/easy-rsa/pki/dh.pem

[root@kali]# ls pki/
ca.crt dh.pem index.txt.attr openssl-easyrsa.cnf renewed revoked serial
certs_by_serial index.txt issued private reqs safessl-easyrsa.cnf

[root@kali]# cat pki/dh.pem
-----BEGIN DH PARAMETERS-----
MIIBCAKCAQEAqLsgXHu2TM3+8AKVYXwOquar/BsLJ3A7H40uc055ActQny1JEyhV
PD8saMfy8pHJAjb428ihU1bUca0Hls2hqaCscPspHi6zyEUktQf7QEmiTgNGWd95
fvY/pMBy/skRVnhn1lQ9LyvE82RM+wZqPpvmeBtIR1MqQuwD002k1F7y4Qqaxb
0+Dz9LYB8voCsgVmrbNk1kmJYdnJXUrN27x2/Z7hnFQQK156sL2G19cV+4uq+FY
+EoLx/M1Z/KFxQJ7ntocR1RHFSUpeSwUbsoPzI5Ty4nGJW6cg9yXcz0JnUkwqoDv
eum2d17jFRAvvslQxEYIb3dkReZA4NBx7gwIBAg=
-----END DH PARAMETERS-----

[root@kali]#
```

```
Kali_Linux_Server | Ubuntu_Linux_Client
root@kali: /etc/openvpn/...
root@kali: /etc/openvpn/easy-rsa
Fichier Actions Éditer Vue Aide
[root@kali]# ./easyrsa gen-req INSAT nopass
Using SSL: openssl OpenSSL 1.1.1l 24 Aug 2021
Generating an RSA private key
.....+
.....+
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa/4626.tAFUC0/tmp.NphU7b'

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) [INSAT]:www.insat.tn

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/INSAT.req
key: /etc/openvpn/easy-rsa/pki/private/INSAT.key

[root@kali]# cat pki/reqs/INSAT.req
-----BEGIN CERTIFICATE REQUEST-----
MIICXDCCAUQCQAwFzEVMBGAUEAwMd3d3Lmluc2F0LnRuMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIIBCgKCAQEAYyMvOMo8ucmrvfsWcymWj3t92tXAIDAX2nk
5gAj9ln62qycCc12+FprIWCG8huafUk1gJDw045t2/9hfefq+nsZ0GU1LnYudGNL
OxfCl+it/2LufunDbFofpgB20LZUTAFmUgJGgZlqp/nv6Rnf+10ax3noVd0aU0WR
gMwZnPrS0sc2nm0KbcCY7bVw3Q9UYlesTC7Xu4NHHiixmsjMb/L9BxVL46RqXzod
```



```
Kali_Linux_Server x Ubuntu_Linux_Client x
[  root@kali: /etc/openvpn/...
root@kali:/etc/openvpn/easy-rsa

Fichier Actions Éditer Vue Aide

MIICXDCCAQAwFzEVMBMGA1UEAwMd3d3Lmluc2F0LnRuMIIIBIjANBgkqhkiG
9wBAQFEAAOCQA8AMIBiCgKCAQeAYEvMo8ucmrvfsWcmWj3t92xALDAZknk
5qAj0ln6n2yCcg12+PprIWG8huAFUk1gJw0@452z/Hffgf+nsZ0GUinNyudGNL
0xfCl+it+2LufunDboFpgB20LZUTAFmJgJgZlp/nuGrF+10ax3novd0aU0WR
gMwZnPrS0c2m@0KbcCY7bVw3Q9UYulesTC7Xu4NWHiiixnsjMb/L98xVL46RqXzod
eSa17KmENzYON1kFyh1v4u0+AWJk3U2NyKaczk38KM9uA8HBeMh8ZzbPC0tueia
FEd2npJwn2c20xr3Dq+0Zmbw+rpOBHuf0H2M1avwXhiKvIDQBaAwDQYJ
Ko2InhcNAQELBQADggEBABQPeafSPpdZ0LzLXFtJzr1bJg3xtiulGWp5pSyl
lRISpHx/K6YgdRTKRJtJF7NHfC166nshM3N1e40AOEfujC3G0hMcNrJlHea
KNgA-pxTtuAf94ok3Y4V/eZmXnwsoNjKuiyu-/luMuzxiniFdgJfbjaVNjrywUI
7iivrsevZlC70EV/UmOAKHOfzXlQ96g5lZ5YnpzYLE3TTpVKRwKKNs/eJ9tXoc9
ZYD4noW8ajwyKuuJuiVUmtrMRV2o15pTBcluqqSbfXifATD6j+VVNbh4NzK/7GU
CfufPMZtGsuNHNxpCjQKMKhRe=1oVLVtBK2OPD8c0=
-----END CERTIFICATE REQUEST-----

[  root@kali: /etc/openvpn/easy-rsa]
# ./easyrsa sign-req server INSAT
Using SSL: openssl OpenSSL 1.1.1 24 Aug 2021

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a server certificate for 825 days:

subject=
  commonName      = www.insat.tn

Type the word 'yes' to continue, or any other input to abort.
```

```
Kali_Linux_Server x Ubuntu_Linux_Client x
root@kali:/etc/openvpn/...
root@kali:/etc/openvpn/easy-rsa

Fichier Actions Éditer Vue Aide
Request subject, to be signed as a server certificate for 825 days:
subject=commonName = www.insat.tn

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-4663.88L1QM/tmp.7kjcQ6
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'www.insat.tn'
Certificate is to be certified until Apr 1 01:23:59 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/INSAT.crt

[root@kali]~# openssl x509 -in pki/issued/INSAT.crt -subject -issuer -dates -noout
subject=CN = www.insat.tn
issuer=CN = Easy-RSA CA
notBefore=Dec 28 01:23:59 2021 GMT
notAfter=Apr 1 01:23:59 2024 GMT

[root@kali]~#
```



Kali Linux Server | Ubuntu Linux Client | root@kali:/etc/openvpn/... | 02:40 AM

```
(root㉿kali)-[~/etc/openvpn/easy-rsa]
# cp pki/dh.pem pki/ca.crt pki/issued/INSAT.crt pki/private/INSAT.key /etc/openvpn/
[root@kali ~]# cd ..
[root@kali ~]# ls
ca.crt dh.pem easy-rsa INSAT.crt INSAT.key server.txt serveur.txt
[root@kali ~]# cd easy-rsa/
[root@kali ~]# ls
easyrsa openssl-easyrsa.cnf pki vars x509-types
[root@kali ~]#
```

Maintenant on va passer au client

Kali Linux Server | Ubuntu Linux Client | root@kali:/etc/openvpn/... | 02:44 AM

```
(root㉿kali)-[~/etc/openvpn/easy-rsa]
# ./easyrsa gen-req lola nopass
Using SSL: openssl OpenSSL 1.1.1l 24 Aug 2021
Generating a RSA private key
+++++
writing new private key to '/etc/openvpn/easy-rsa/pki/easy-rsa-4841.ll1eq6/tmp.SUrDkc'

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) [lola]:
```

Keypair and certificate request completed. Your files are:
req: /etc/openvpn/easy-rsa/pki/reqs/lola.req
key: /etc/openvpn/easy-rsa/pki/private/lola.key

```
[root@kali ~]# ./easyrsa sign-req client lola
Using SSL: openssl OpenSSL 1.1.1l 24 Aug 2021

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
```



Kali_Linux_Server × Ubuntu_Linux_Client ×

root@kali:/etc/openvpn/...

root@kali:/etc/openvpn/easy-rsa

Fichier Actions Éditer Vue Aide

You are about to sign the following certificate.
Please check over the details shown below for accuracy. Note that this request
has not been cryptographically verified. Please be sure it came from a trusted
source or that you have verified the request checksum with the sender.

Request subject, to be signed as a client certificate for 825 days:

subject=

 commonName = lola

Type the word 'yes' to continue, or any other input to abort.
Confirm request details: yes
Using configuration from /etc/openvpn/easy-rsa/pki/easy-rsa-4866.5Rr622/tmp.e1cfwH
Enter pass phrase for /etc/openvpn/easy-rsa/pki/private/ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
commonName :ASN.1 12:'lola'
Certificate is to be certified until Apr 1 01:44:34 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /etc/openvpn/easy-rsa/pki/issued/lola.crt

(root㉿kali)-[~/Documents]

```
Kali_Linux_Server x Ubuntu_Linux_Client x
root@kali: /etc/openvpn/...
root@kali:/etc/openvpn/easy-rsa/pki

Fichier Actions Éditer Vue Aide

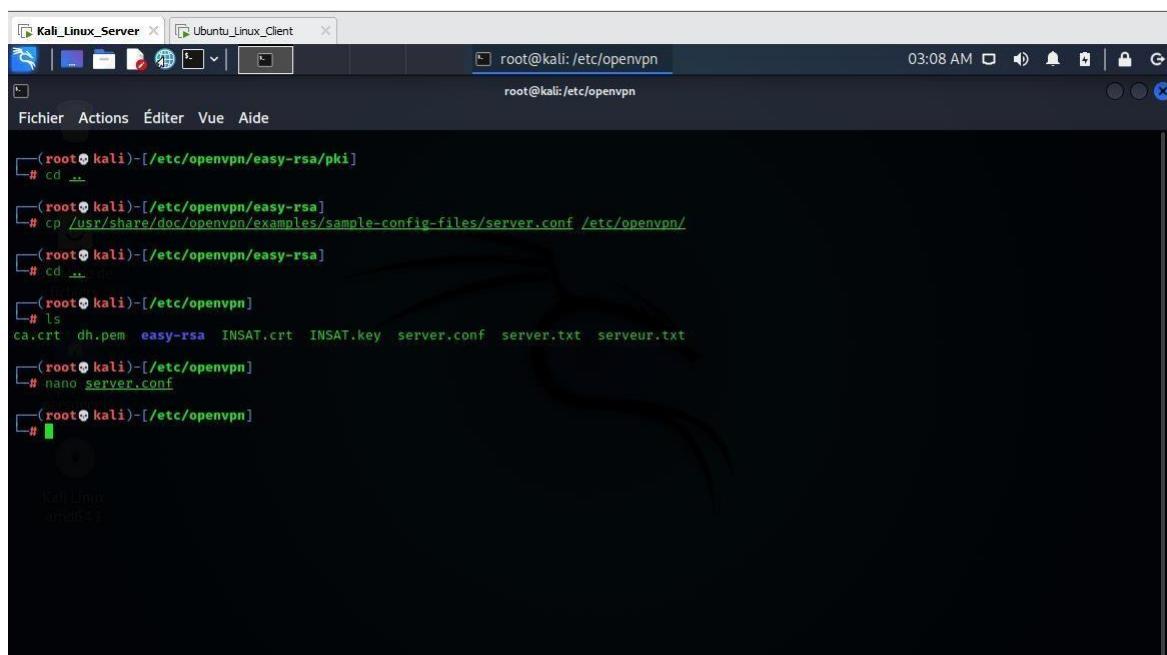
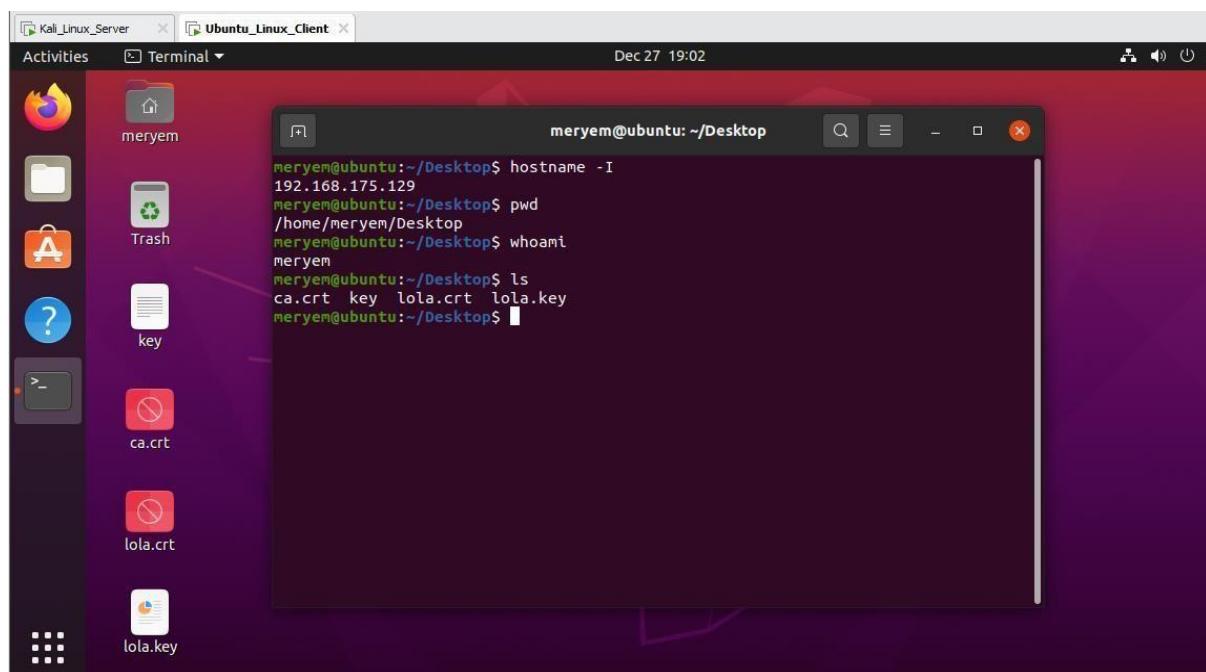
└─[root@kali-/etc/openvpn/easy-rsa]
# ls
easyrsa openssl-easyrsa.cnf pki vars x509-types

└─[root@kali-/etc/openvpn/easy-rsa]
# cd pki/
└─[root@kali-/etc/openvpn/easy-rsa/pki]
# ls issued/
INSAT.crt lola.crt

└─[root@kali-/etc/openvpn/easy-rsa/pki]
# ls private/
ca.key INSAT.key lola.key

└─[root@kali-/etc/openvpn/easy-rsa/pki]
# scp ca.crt issued/lola.crt private/lola.key meryem@192.168.175.129:/home/meryem/Desktop
meryem@192.168.175.129's password:
ca.crt          100% 1204    105.4KB/s  00:00
lola.crt        100% 4486     1.2MB/s  00:00
lola.key        100% 1708    788.0KB/s  00:00

└─[root@kali-/etc/openvpn/easy-rsa/pki]
#
```





Kali_Linux_Server X Ubuntu_Linux_Client X

root@kali:/etc/openvpn

03:06 AM

Fichier Actions Éditer Vue Aide

GNU nano 5.9 server.conf

```
#####
# Sample OpenVPN 2.0 config file for
# multi-client server.
#
# This file is for the server side
# of a many-clients ↔ one-server
# OpenVPN configuration.
#
# OpenVPN also supports
# single-machine ↔ single-machine
# configurations (See the Examples page
# on the web site for more info).
#
# This config should work on Windows
# or Linux/BSD systems. Remember on
# Windows to quote pathnames and use
# double backslashes, e.g.:
# "C:\\Program Files\\OpenVPN\\config\\foo.key"
#
# Comments are preceded with '#' or ';'
#####

# Which local IP address should OpenVPN
# listen on? (optional)
;local a.b.c.d

# Which TCP/UDP port should OpenVPN listen on?
# If you want to run multiple OpenVPN instances
# on one machine you can assign multiple ports here
# (see man page)

#dev-node MyTap
```

Aide Écrire Chercher Couper Exécuter Emplacement Annuler Marquer → Crochet Quitter Lire fich. Remplacer Coller Justifier Aller ligne Refaire Copier Retrouver

Kali_Linux_Server X Ubuntu_Linux_Client X

root@kali:/etc/openvpn

03:19 AM

Fichier Actions Éditer Vue Aide

GNU nano 5.9 server.conf *

```
#####
# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key). Each client
# and the server must have their own cert and
# key file. The server and all clients will
# use the same ca file.
#
# See the "easy-rsa" directory for a series
# of scripts for generating RSA certificates
# and private keys. Remember to use
# a unique Common Name for the server
# and each of the client certificates.
#
# Any X509 key management system can be used.
# OpenVPN can also use a PKCS #12 formatted key file
# (see "pkcs12" directive in man page).
ca /etc/openvpn/ca.crt
cert /etc/openvpn/INSAT.crt
key /etc/openvpn/INSAT.key # This file should be kept secret

# Diffie hellman parameters.
# Generate your own with:
#   openssl dhparam -out dh2048.pem 2048
dh /etc/openvpn/dh.pem

# Network topology
# Should be subnet (addressing via IP)
```

Aide Écrire Chercher Couper Exécuter Emplacement Annuler Marquer → Crochet Quitter Lire fich. Remplacer Coller Justifier Aller ligne Refaire Copier Retrouver



```
# nano server.conf
# openvpn --genkey secret ta.key
# ls
ca.crt dh.pem easy-rsa INSAT.crt INSAT.key server.conf server.txt serveur.txt ta.key
# cat ta.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
d387a28edc040a8e1d88ea95b1874af
34b790e13c4cfb746d7b42d12c8ea7b7
cf133b6036e732d38a1ee191bc2b14
702f973ec3f1e4951623c36fccc0318
d362996ad132dccfc7b9e91d33f856aa
90a915b7fab466cc62ccb803aa488dbaa
3e75c14fcfd820546be1ac76c0ccb978
d08001d667f2cfdd0a6f674a8aa3a7789
531e0f17f636ca2e1b66953e39815f7
0214f3727c4c467ca71fbfc877a48702
468d3d675b2377cd0572d8098e2851a
59203e3927930c31471e7bfefdf49bf
d493397702973e8f46b1a2deaad74d40
7ed30b30755d5eac2be5b095fbcc1e53
538a60c4ab91ecbc1f60df5f3dcfe0c
3f8f81ec35daaffb261c4a14ce7457a9
-----END OpenVPN Static key V1-----
```

```
# nano /etc/svcs.conf
# nano /etc/openvpn
```



Kali_Linux_Server X Ubuntu_Linux_Client X

root@kali:/etc/openvpn

03:28 AM

Fichier Actions Éditer Vue Aide

```
GNU nano 5.9 /etc/sysctl.conf *
```

```
# /etc/sysctl.conf - Configuration file for setting system variables
# See /etc/sysctl.d/ for additional system variables.
# See sysctl.conf (5) for information.

#
#kernel.domainname = example.com

# Uncomment the following to stop low-level messages on console
#kernel.printk = 3 4 1 3

#####
# Functions previously found in netbase
#

# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#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
```

Aide Écrire Chercher Couper Exécuter Emplacement Annuler Marquer → Crochet Quitter Lire fich. Remplacer Coller Justifier Aller ligne Refaire Copier Retrouver

Kali_Linux_Server X Ubuntu_Linux_Client X

root@kali:/etc/openvpn

03:36 AM

Fichier Actions Éditer Vue Aide

Use --help for more information.

```
(root@kali)-[~/etc/openvpn]
# openvpn /etc/openvpn/server.conf
2021-12-28 03:33:06 WARNING: --topology net30 support for server configs with IPv4 pools will be removed in a future release. Please migrate to
o --topology subnet as soon as possible.
2021-12-28 03:33:06 DEPRECATED OPTION: --cipher set to 'AES-256-CBC' but missing in --data-ciphers (AES-256-GCM:AES-128-GCM). Future OpenVPN v
ersion will ignore --cipher for cipher negotiations. Add 'AES-256-CBC' to --data-ciphers or change --cipher 'AES-256-CBC' to --data-ciphers-fa
llback 'AES-256-CBC' to silence this warning.
2021-12-28 03:33:06 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-12-28 03:33:06 library versions: OpenSSL 1.1.1l 24 Aug 2021, LZO 2.10
2021-12-28 03:33:06 net_route_v4_best_gw query: dst 0.0.0.0
2021-12-28 03:33:06 net_route_v4_best_gw result: via 192.168.175.2 dev eth0
2021-12-28 03:33:06 Diffie-Hellman initialized with 2048 bit key
2021-12-28 03:33:06 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2021-12-28 03:33:06 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
2021-12-28 03:33:06 net_route_v4_best_gw query: dst 0.0.0.0
2021-12-28 03:33:06 net_route_v4_best_gw result: via 192.168.175.2 dev eth0
2021-12-28 03:33:06 ROUTE_GATEWAY 192.168.175.2/255.255.255.0 IFACE=eth0 HWADDR=00:0c:29:25:1c:b5
2021-12-28 03:33:06 TUN/TAP device tun0 opened
2021-12-28 03:33:06 net_iface_mtu_set: mtu 1500 for tun0
2021-12-28 03:33:06 net_iface_up: set tun0 up
2021-12-28 03:33:06 net_addr_ptp_v4_add: 10.8.0.1 peer 10.8.0.2 dev tun0
2021-12-28 03:33:06 net_route_v4_add: 10.8.0.0/24 via 10.8.0.2 dev [NULL] table 0 metric -1
2021-12-28 03:33:06 Could not determine IPv4/IPv6 protocol. Using AF_INET
2021-12-28 03:33:06 Socket Buffers: R=[212992→212992] S=[212992→212992]
2021-12-28 03:33:06 TCP/UDP: Socket bind failed on local address [AF_INET][undefined]:1194: Address already in use (errno=98)
2021-12-28 03:33:06 Exiting due to fatal error
2021-12-28 03:33:06 net_route_v4_del: 10.8.0.0/24 via 10.8.0.2 dev [NULL] table 0 metric -1
2021-12-28 03:33:06 Closing TUN/TAP interface
2021-12-28 03:33:06 net_addr_ptp_v4_del: 10.8.0.1 dev tun0
```



```
meryem@kali:~$ hostname -I
192.168.175.128 192.168.175.130 10.0.0.1
meryem@kali:~$
```

```
root@kali:/etc/openvpn
# cd /easy-rsa/
cd: aucun fichier ou dossier de ce type: /easy-rsa/
[root@kali]~[~/etc/openvpn]
# ls
ca.crt dh.pem easy-rsa INSAT.crt INSAT.key server.conf server.txt serveur.txt ta.key
[root@kali]~[~/etc/openvpn]
# cd /easy-rsa
cd: aucun fichier ou dossier de ce type: /easy-rsa/
[root@kali]~[~/etc/openvpn]
# cd easy-rsa/
[root@kali]~[~/etc/openvpn/easy-rsa]
# ls
easyrsa openssl-easyrsa.cnf pki vars x509-types
[root@kali]~[~/etc/openvpn/easy-rsa]
# cd ..
[root@kali]~[~/etc/openvpn]
# ls
ca.crt dh.pem easy-rsa INSAT.crt INSAT.key server.conf server.txt serveur.txt ta.key
[root@kali]~[~/etc/openvpn]
# scp ta.key meryem@192.168.175.129:/home/meryem/Desktop
meryem@192.168.175.129's password:
ta.key
[root@kali]~[~/etc/openvpn]
```



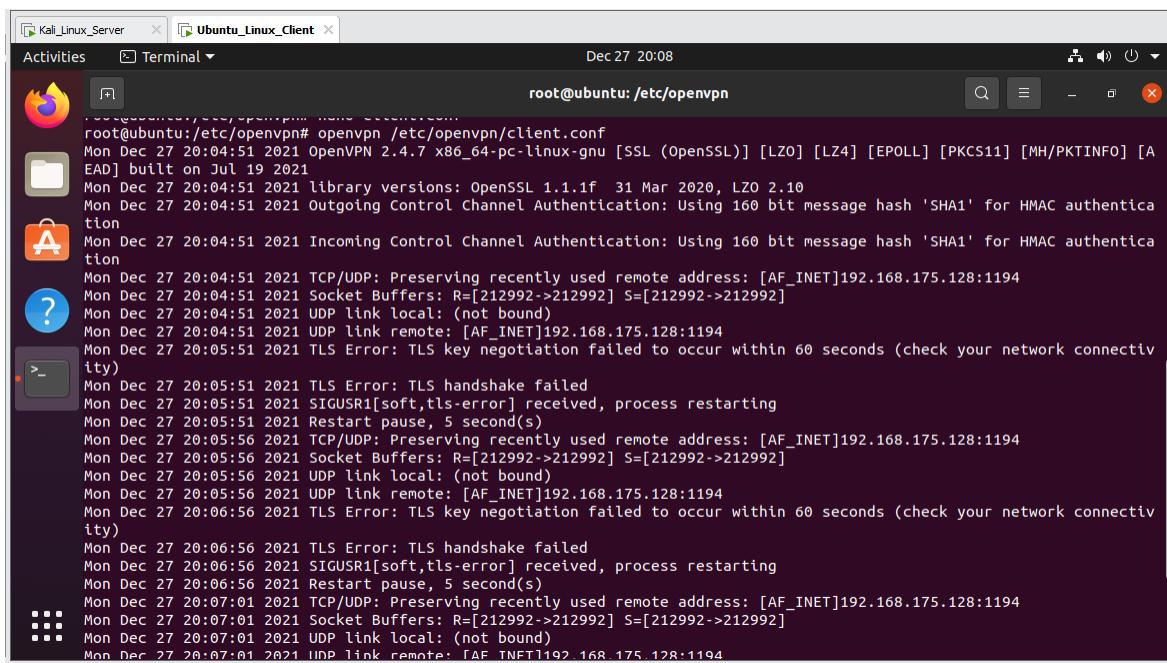
```
meryem@ubuntu:~/Desktop$ hostname -I
192.168.175.129
meryem@ubuntu:~/Desktop$ pwd
/home/meryem/Desktop
meryem@ubuntu:~/Desktop$ whoami
meryem
meryem@ubuntu:~/Desktop$ ls
ca.crt key lola.crt lola.key
meryem@ubuntu:~/Desktop$ ls
ca.crt key lola.crt lola.key ta.key
meryem@ubuntu:~/Desktop$ sudo cp ca.crt lola.crt lola.key ta.key /etc/openvpn
[sudo] password for meryem:
meryem@ubuntu:~/Desktop$ sudo su
root@ubuntu:/home/meryem/Desktop# cd /etc/openvpn/
root@ubuntu:/etc/openvpn# ls
ca.crt client lola.crt lola.key server ta.key update-resolv-conf
root@ubuntu:/etc/openvpn# cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
cp: missing destination file operand after '/usr/share/doc/openvpn/examples/sample-config-files/client.conf'
Try 'cp --help' for more information.
root@ubuntu:/etc/openvpn# cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf .
root@ubuntu:/etc/openvpn# ls
ca.crt client.conf lola.key ta.key
client lola.crt server update-resolv-conf
root@ubuntu:/etc/openvpn# nano client.conf
```

```
GNU nano 4.8                                         client.conf                                         Modified
# file can be used for all clients.
ca /etc/openvpn/ca.crt
cert /etc/openvpn/lola.crt
key /etc/openvpn/client.key

# Verify server certificate by checking that the
# certificate has the correct key usage set.
# This is an important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
#
# To use this feature, you will need to generate
# your server certificates with the keyUsage set to
# digitalSignature, keyEncipherment
# and the extendedKeyUsage to
# serverAuth
# EasyRSA can do this for you.
remote-cert-tls server

# If a tls-auth key is used on the server
# then every client must also have the key.
tls-auth /etc/openvpn/ta.key 1

# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
```



The screenshot shows a terminal window titled "root@ubuntu: /etc/openvpn" running on a Kali Linux Server. The terminal displays log output from an OpenVPN client configuration. The logs show the client connecting to a remote server at 192.168.175.128 port 1194. The connection fails due to TLS errors, specifically "TLS handshake failed" and "SIGUSR1[soft,tls-error] received, process restarting". The client attempts to reconnect multiple times, but the errors persist. The log ends with a UDP link remote entry.

```
root@ubuntu:/etc/openvpn# openvpn /etc/openvpn/client.conf
Mon Dec 27 20:04:51 2021 OpenVPN 2.4.7 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AES-128-GCM] [AES-128-CBC] [SHA256] [SHA1] [BLAKE2] [Vernam] [CAMELLIA] [CHACHA20] [POLY1305] built on Jul 19 2021
Mon Dec 27 20:04:51 2021 library versions: OpenSSL 1.1.1f  31 Mar 2020, LZO 2.10
Mon Dec 27 20:04:51 2021 Outgoing Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Dec 27 20:04:51 2021 Incoming Control Channel Authentication: Using 160 bit message hash 'SHA1' for HMAC authentication
Mon Dec 27 20:04:51 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:04:51 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Dec 27 20:04:51 2021 UDP link local: (not bound)
Mon Dec 27 20:04:51 2021 UDP link remote: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:05:51 2021 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
Mon Dec 27 20:05:51 2021 TLS Error: TLS handshake failed
Mon Dec 27 20:05:51 2021 SIGUSR1[soft,tls-error] received, process restarting
Mon Dec 27 20:05:51 2021 Restart pause, 5 second(s)
Mon Dec 27 20:05:56 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:05:56 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Dec 27 20:05:56 2021 UDP link local: (not bound)
Mon Dec 27 20:05:56 2021 UDP link remote: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:06:56 2021 TLS Error: TLS key negotiation failed to occur within 60 seconds (check your network connectivity)
Mon Dec 27 20:06:56 2021 TLS Error: TLS handshake failed
Mon Dec 27 20:06:56 2021 SIGUSR1[soft,tls-error] received, process restarting
Mon Dec 27 20:06:56 2021 Restart pause, 5 second(s)
Mon Dec 27 20:07:01 2021 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.175.128:1194
Mon Dec 27 20:07:01 2021 Socket Buffers: R=[212992->212992] S=[212992->212992]
Mon Dec 27 20:07:01 2021 UDP link local: (not bound)
Mon Dec 27 20:07:01 2021 UDP link remote: [AF_INET]192.168.175.128:1194
```



CONCLUSION

Actuellement souscrire à un VPN devient une nécessité, puisqu'il présente plusieurs avantages à savoir, être anonyme sur le Net, contourner les restrictions géographiques, télécharger sans être tracé, la prévention contre le piratage des données personnelles, et il est simple à utiliser.

Dans ce contexte, OpenVPN est l'un des protocoles les plus connus, grâce à son haut niveau de sécurité, sa compatibilité avec tous les systèmes d'exploitation, et aussi le fait qu'il est Open Source.



WEBOGRAPHIE

- <https://www.futura-sciences.com/tech/definitions/connection-vpn-1819/>