

SADEK

ADEL

SIO2

IP du client dans le vlan 10 = 172.17.1.26

IP du serveur dans le vlan 50 = 172.19.0.6

J'installe les paquet openvpn wireshark openssl sur le client et serveur

Les options à expliquer

--remote = Le client precise cette option pour préciser l'ip du serveur

--dev = Interface virtuel

--port = préciser port du serveur pour le client et pour le serveur préciser le port utiliser pour ce service

--verb = mode bavard

--ifconfig = Du coté client <IpclientDansLeTunnel> <IpServeurDansleTunnel>

--genkey --secret = générer une clé symétrique pour la communication

--push = Pour envoyer des configurations au client comme des routes,un serveur dns etc

--dh = clé diffie helman

--ca = certificat de l'autorité de certification

--cert = cert certificat du serveur ou du client si authentication par clé du client, certificat = clé publique

--key = la clé privée

Création d'un tunnel non crypter

Sur le serveur je lance cette commande

Openvpn --dev tun0 --verb 5 --ifconfig 10.255.0.1 10.255.0.2

#Ici je définis un tunnel dans une des extrémités sera mon interface tun0 qui sera créer pour cette communication, if config la première ip est l'ip du serveur la seconde et l'ip du client

Sur le client j'exécute ceci

```
Openvpn --dev tun0 --verb 5 --ifconfig 10.255.0.2 10.255.0.1 --remote @IPSERVEURVPN
```

#Pareil ici sur le client son interface tun 0 sera l'autre extrémité après IFCONFIG la première ip est son ip la seconde est celle du serveur vpn

Et remote sa précise l'ip du serveur vpn

Je lance la commande sur le serveur et un gros message warning s'affiche pour prévenir que la connexion n'est pas cryptée etc

```
2021-11-18 16:05:14 us=528089 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOL
[PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2021-11-18 16:05:14 us=528104 library versions: OpenSSL 1.1.1k 25 Mar 2021, LZ0 2.10
2021-11-18 16:05:14 us=528219 ***** WARNING *****: All encryption and authentication features
sabled -- All data will be tunneled as clear text and will not be protected against man-in-the-m
le changes. PLEASE DO RECONSIDER THIS CONFIGURATION!
2021-11-18 16:05:14 us=635777 TUN/TAP device tun0 opened
2021-11-18 16:05:14 us=635822 do_ifconfig, ipv4=1, ipv6=0
2021-11-18 16:05:14 us=635874 net_iface_mtu_set: mtu 1500 for tun0
2021-11-18 16:05:14 us=635922 net_iface_up: set tun0 up
2021-11-18 16:05:14 us=635988 net_addr_ptp_v4_add: 10.255.0.1 peer 10.255.0.2 dev tun0
2021-11-18 16:05:14 us=636043 Data Channel MTU parms [ L:1500 D:1450 EF:0 EB:386 ET:0 EL:3 ]
```

Je fais « ip a » dans un autre terminal et je vois qu'il y'a une interface tun0 qui s'est créé avec mon ip et celle du client en mode connexion PPP

```
valid_lft forever preferred_lft forever
tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
UNKNOWN group default qlen 500
    link/none
    inet 10.255.0.1 peer 10.255.0.2/32 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::d8b2:1c7c:2dfc:90b9/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
```

J'exécute maintenant la commande sur le serveur

```
LZO 2.10
2021-11-18 10:08:21 us=411397 ***** WARNING *****: All encryption and aut
hentication 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!
2021-11-18 10:08:21 us=609448 TUN/TAP device tun0 opened
2021-11-18 10:08:21 us=609471 do_ifconfig, ipv4=1, ipv6=0
2021-11-18 10:08:21 us=609500 net_iface_mtu_set: mtu 1500 for tun0
2021-11-18 10:08:21 us=609530 net_iface_up: set tun0 up
2021-11-18 10:08:21 us=609615 net_addr_ptp_v4_add: 10.255.0.2 peer 10.255.0.1
dev tun0
```

Pareil le message s'affiche

Je tape la commande « ip a » pour voir si l'interface virtuel a été créer et que l'ip a bien été prise

L'interface a correctement été créer

```
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc
state UNKNOWN group default qlen 500
    link/none
    inet 10.255.0.2 peer 10.255.0.1/32 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::26b:4931:d1fd:56a3/64 scope link stable-privacy
        valid_lft forever preferred_lft forever
```

Du coté serveur on voit que la connexion a été initialiser

```
2021-11-18 16:05:14 us=636093 UDPv4 link remote: [AF_UNSPEC]
rrrrrr2021-11-18 16:09:09 us=527767 Peer Connection Initiated with [AF_INET]172.17.1.26:1194
2021-11-18 16:09:09 us=527864 WARNING: this configuration may cache passwords in memory -- use the
uth-nocache option to prevent this
```

J'essaye de ping 10.255.0.1 qui est l'ip du serveur vpn depuis le client

```
64 bytes from 10.255.0.1: icmp_seq=24 ttl=64 time=1.88 ms
64 bytes from 10.255.0.1: icmp_seq=25 ttl=64 time=2.45 ms
64 bytes from 10.255.0.1: icmp_seq=26 ttl=64 time=2.47 ms
64 bytes from 10.255.0.1: icmp_seq=27 ttl=64 time=2.60 ms
64 bytes from 10.255.0.1: icmp_seq=28 ttl=64 time=2.27 ms
64 bytes from 10.255.0.1: icmp_seq=29 ttl=64 time=2.54 ms
64 bytes from 10.255.0.1: icmp_seq=30 ttl=64 time=1.72 ms
64 bytes from 10.255.0.1: icmp_seq=31 ttl=64 time=2.46 ms
64 bytes from 10.255.0.1: icmp_seq=32 ttl=64 time=1.92 ms
64 bytes from 10.255.0.1: icmp_seq=33 ttl=64 time=2.39 ms
```

Sa fonctionne

Sur le serveur je lance un wireshark sur mon interface eth0 voici ce que je vois

Je vois clairement le contenu de la trame

No.	Time	Source	Destination	Protocol	Length	Info
17	6.238672800	172.17.1.26	172.19.0.6	OpenVPN	126	MessageType
18	6.238788500	172.19.0.6	172.17.1.26	OpenVPN	126	MessageType
19	6.409508300	172.17.1.26	172.19.0.6	OpenVPN	90	MessageType

Frame 17: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface eth0,
Interface id: 0 (eth0)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 18, 2021 16:39:18.799495200 CET
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1637249958.799495200 seconds
[Time delta from previous captured frame: 0.534772800 seconds]
[Time delta from previous displayed frame: 0.534772800 seconds]
[Time since reference or first frame: 6.238672800 seconds]

```
0000  00 15 5d 13 25 06 ac f2 c5 48 ac 20 08 00 45 00  ..].%...H...E.
0010  00 70 35 43 40 00 3f 11 ac f5 ac 11 01 1a ac 13  ..p5C@.?.
0020  00 06 04 aa 04 aa 00 5c 9c 9d 45 00 00 54 99 d4  .....\\...E..T..
0030  40 00 40 01 8a d4 0a ff 00 02 0a ff 00 01 08 00  @.@.....
0040  c4 43 5c 04 00 04 76 73 96 61 00 00 00 00 ff 0b  .C\...vs.a.....
0050  0d 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19  .....
0060  1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29  .....["#%&'()
0070  2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 36 37      *+,-./01 234567
```

Je coupe la communication sur le serveur et client et je lance la commande

Openvpn --genkey --secret <fichier> sur le serveur vpn

```
root@OPENVPN:~# openvpn --genkey --secret cle.key
2021-11-18 16:18:12 WARNING: Using --genkey --secret filename is DEPRECATED. Use
lename instead.
root@OPENVPN:~# cat cle.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
2f8ca802d9d86bca56db5936f1ca9dcd
488d43b3ac6879fb77dd602a7e5adec7
130a4e6538600637b859194305aeeb5d
e1faece2108d2d6d8c7edeee04dc006a
0e6b7dbda7be5db2c814e697a3198406
7721bf55bfc23f0fdede955b52efd973
71d55ccf9534bcabf86339312ed1fa9b
5a7015a3133a2e1fb0f2c47219a5189d
fbb4af02ffe9d47a11681051d0508f58
6e3b987d79f9ed278ae59f52273aaa05
153ddb4204c5703a4ca905daf3a0cec4
3531e9a4d0c0f1eeebf9209efd94d39
19e9a5339d02f0397d5fb5594304ec43
719bab81a39fb128853d65c4443a9477
3fb1f3770e90def615b3a67ca25eb73c
df760d081687dff5d190655d3bcb47df
```

Voici le résultat une clé sur 2048 bit c'est correct j'exporte cette clé via scp sur mon client vpn

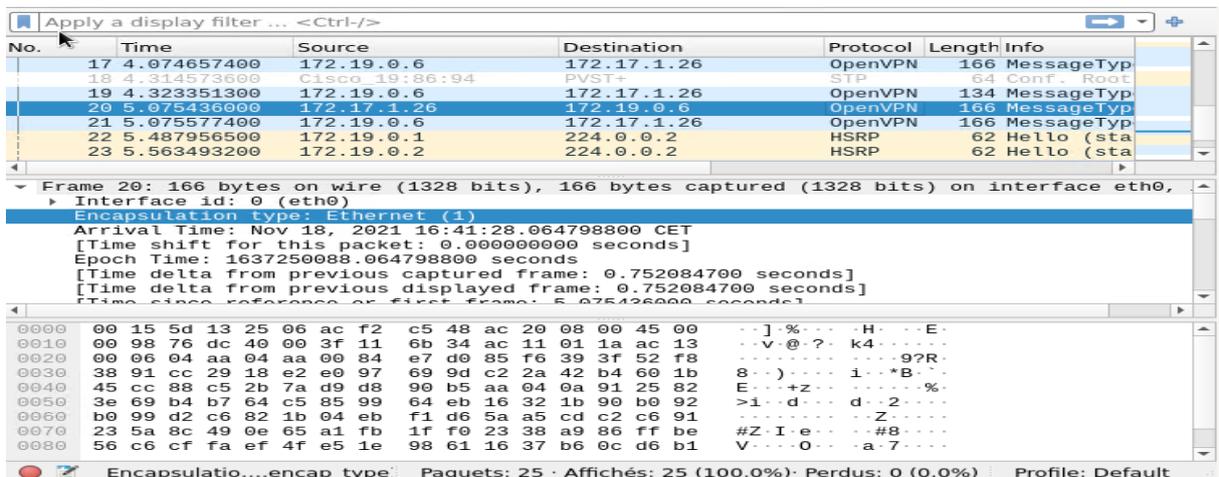
La clé maintenant transporter via scp je relance la connexion et sur le serveur et client je rajoute comme argument --secret <fichierClée>

Il n'ya plus ce message d'alerte comme quoi le trafic n'est pas crypter lorsque que j'ai relancer la communication du srveur et client

Je vais demarrer le serveur et capturer les paquets sur son interface virtuel avant que le client ce connecte pour capturer le moment de la connexion

Ne pas oublier de bien regler les droits sur les clé en cas d'erreur

C'est crypter l'interieur est crypter et je ne peux même pas identifier quel protocole est entrain de transiter dans le tunnel



Création de certificat openssl

Sur le serveur je crée les fichiers

`/apps/openvpn/{log,keys,conf,pki-booktic}`

Je copie ensuite le repertoire easy-rsa dans le dossier pki-booktic

```
openvpn@easyrsa:~/easy-rsa$ cp -r /usr/share/easy-rsa/ /apps/openvpn/pki-booktic/
root@OPENVPN:/apps/openvpn#
```

Il va falloir créer un couple de clé publique(certificat)/clé privée pour :

- La CA
- Le serveur
- Le client openvpn

Je vais dans le fichier `/apps/pki-booktic/vars` et je modifie les valeurs en fonction de mon infrastructure

```
set_var EASYRSA_REQ_COUNTRY      "FR"
set_var EASYRSA_REQ_PROVINCE     "Paris"
set_var EASYRSA_REQ_CITY         "Paris"
set_var EASYRSA_REQ_ORG          "Copyleft Certificate Co"
set_var EASYRSA_REQ_EMAIL        "admin"
set_var EASYRSA_REQ_ORG          "Booktic"
```

Je me déplace dans `/apps/pki-booktic/easy-rsa` et je vais utiliser les scripts easy-rsa pour générer ses clés

Je dois taper la commande `./easyrsa init-pki` avant d'exécuter ses commandes

Pour les clés de la CA je tape : `./easyrsa build-ca nopass`

Après avoir exécuté la commande voilà ce qui s'affiche

```
root@OPENVPN:/apps/openvpn/pki-booktic# ./easysrsa build-ca nopass
Note: using Easy-RSA configuration from: /apps/openvpn/pki-booktic/vars
Using SSL: openssl OpenSSL 1.1.1k 25 Mar 2021
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.booktic.info
CA creation complete and you may now import and sign cert requests.
Your new CA certificate file for publishing is at:
/apps/openvpn/pki-booktic/pki/ca.crt
root@OPENVPN:/apps/openvpn/pki-booktic#
```

La clé pub du Ca est dans le dossier pki créer apres la commande init pki

J'exécute ensuite la commande pour créer le certificat du serveur et client

`./easysrsa gen-req MONSRV nopass`

`./easysrsa gen-req MONCLT nopass`

```
Keypair and certificate request completed. Your files are:
req: /apps/openvpn/pki-booktic/pki/reqs/monsrv.req
key: /apps/openvpn/pki-booktic/pki/private/monsrv.key
```

Ensuite on voit que la clé publique son extension est en « .req » sa veut dire qu'elle attend une signature d'une autorité de certif

Pareil pour le client

Je fais signer la clé du serveur par l'autorité de certification et client comme ceci

`./easysrsa sign-req server MONSRV`

`./easysrsa sign-req client MONCLT`

Il faut ensuite taper yes et on a le certificat signer qui sera generer

```
Signature on
The Subject's Distinguished Name is as follows
CommonName      :ASN.1 12:'openvpn.booktic.info'
Certificate is to be certified until Feb 22 02:19:26 2024 GMT (825 days)

Write out database with 1 new entries
Data Base Updated

Certificate created at: /apps/openvpn/pki-booktic/pki/issued/monsrv.crt
```

Pareil pour le client

Je crée une clé diffiehelman

```
./easyrsa gen-dh
```

Ensuite je crée une signature électronique pour authentifier le client et serveur que je transporterai dans le répertoire « keys »

```
Openvpn --genkey --secret /apps/openvpn/keys/bookticsign.key
```

Ensuite je copie le certificat du CA, la clé DH, certificat et clé serveur dans le répertoire keys

Dans issued il y'a les certificats et les clés privées

Voilà le contenu du répertoire keys

```
root@OPENVPN:/apps/openvpn/pki-booktic/pki/private# cd /apps/openvpn/keys/
root@OPENVPN:/apps/openvpn/keys# ls
bookticsign.key  ca.crt  dh.pem  monsrv.crt  monsrv.key
root@OPENVPN:/apps/openvpn/keys#
```

Je vais dans le répertoire conf et je crée le fichier booktic.conf dans /apps/openvpn/conf

Voici le contenu de ce fichier

```
ca /apps/openvpn/keys/ca.crt
cert /apps/openvpn/keys/monsrv.crt
key /apps/openvpn/keys/monsrv.key
dh /apps/openvpn/keys/dh.pem
tls-auth /apps/openvpn/keys/bookticsign.key

server 10.0.0.0 255.255.255.0
push "route 172.19.0.0 255.255.255.0"

client-to-client

explicit-exit-notify 1
keepalive 10 120
persist-key
persist-tun

cipher AES-256-CBC
compress lz4-v2
status openvpn-status.log
log /apps/openvpn/log/openvpnlog
log-append /apps/openvpn/log/openvpnlog
verb 5
```

Ne pas oublier de préciser :

Proto udp

Dev tun

Je crée le lien symbolique comme demandé

J'active le service mais dans les logs il s'allume en mode strating et apres il marque finished mais le service reste actif je ne comprend pas trop

Config du client :

Je transfere le crt du ca la clé et crt du client vers le client avec scp

Je transfere aussi la signature électronique

Je crée maintenant le fichier de conf du client

Pareil dans le repertoire conf ensuite lien symbolique

```
client
dev tun
proto udp
remote 172.19.0.6 1194
resolv-retry infinite
nobind

persist-key
persist-tun
mute-replay-warnings

ca /apps/openvpn/keys/ca.crt
cert /apps/openvpn/keys/monclt.crt
key /apps/openvpn/keys/monclt.key
tls-auth /apps/openvpn/keys/bookticsign.key

cipher AES-256-CBC
compress lz4-v2
verb 5
```

Pour activer la configuration il faut executer cette commande

Systemctl restart openvpn@confServer (mettre nom du fichier sans .conf)

Ce message d'erreur ne cesse de s'afficher dans les logs du serveur

```
Nov 19 04:13:57 ServeurNagios systemd[1]: openvpn@booktic.conf.service: Process exited with code
ited, status=1/FAILURE
Nov 19 04:13:57 ServeurNagios systemd[1]: openvpn@booktic.conf.service: Failed with result 'exit-co
e'.
Nov 19 04:13:57 ServeurNagios systemd[1]: Failed to start OpenVPN connection to booktic.conf.
```

J'ai commenté la directive push route sur le serveur j'ai redémarré le service avec la commande vu plus haut sur les deux serveurs et la connexion c'est directement effectuée le serveur VPN à cette IP dans le réseau 10.0.0.1 et mon client 10.0.0.5

Dev tun = utiliser l'interface tun

Persist-tun = persistance du tunnel

Cipher AES ... = Type de cryptage symetrique supporté

Compress = le trafic sera compresser

explicit-exit-notify : le serveur sera a notifié quand vous vous déconnecterez

resol-retry-infinite : essayer de ce connecter infiniment

nobind : Pas besoin de se lier a un port local

Mise en place du routage et natting

L'option push « redirect-gateway def1 » permet de faire en sorte que la passerelle par défaut sois le serveur vpn que aucun trafic des clients ne passent par autre que le tunnel

Sur pfsense je desactive le pare-feu sans desactiver le nat

Sur l'interface admin vlan 30

Je crée une regle qui autorise tout le trafic venant de n'importe ou avec n'importe quel port et protocole

Sur interface wan vlan 60 pareil

Sur mon client vpn je me met sur la salle et demande une ip via dhcp

Mon ip sera la 172.16.19.13

Je vais essayer de ping mon serveur d'abord je definis une route que pour aller vers le vlan 50 je dois passer par le pfsense

Comme ceci et le ping passe bien

```
(root@kali)~# ip route add 172.19.0.0/24 via 172.16.19.70 dev eth0

(root@kali)~# ping 172.16.19.70
PING 172.16.19.70 (172.16.19.70) 56(84) bytes of data:
64 bytes from 172.16.19.70: icmp_seq=1 ttl=64 time=0.867 ms
64 bytes from 172.16.19.70: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.16.19.70: icmp_seq=3 ttl=64 time=0.989 ms
64 bytes from 172.16.19.70: icmp_seq=4 ttl=64 time=0.586 ms
^C
--- 172.16.19.70 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 0.455/0.724/0.989/0.213 ms
```

Et le ping entre le client vpn et le serveur vpn passe correctement

```
(root@kali)~# ping 172.19.0.5
PING 172.19.0.5 (172.19.0.5) 56(84) bytes of data:
64 bytes from 172.19.0.5: icmp_seq=1 ttl=62 time=3.18 ms
64 bytes from 172.19.0.5: icmp_seq=2 ttl=62 time=2.73 ms
64 bytes from 172.19.0.5: icmp_seq=3 ttl=62 time=2.11 ms
64 bytes from 172.19.0.5: icmp_seq=4 ttl=62 time=2.35 ms
^C
--- 172.19.0.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.114/2.593/3.178/0.402 ms
```

Maintenant je vais dans /etc/sysctl.conf sur mon serveur et j'active le routage et remarque le service procs

Et je configure le nat comme ceci

```
valid ttl forever preferred ttl forever
root@OPENVPN:/var/log/openvpn# iptables -t nat -A POSTROUTING -o eth0 -s 10.0.0.0/24 -j MASQUERADE
root@OPENVPN:/var/log/openvpn#
```

Bien préciser dans la source le réseau

Je vais maintenant faire une redirection de port une règle de PAT sur mon pare-feu sense qui redirigera les requêtes vers le port 1194 de son interface WAN vers le port 1194 en udp du serveur vpn

Voilà la règle

Règles										
<input type="checkbox"/>	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP/UDP	*	*	WAN address	1194 (OpenVPN)	172.19.0.5	1194 (OpenVPN)	Serveur Openvpn Adel	 

Je modifie la directive remote sur mon client vpn pour qu'il envoie la requete de connexion openvpn etc sur le port 1194 de l'interface WAN du pfsense qui lui renverra sa vers mon serveur VPN son port 1194

```
client
dev tun
proto udp
remote 172.16.19.70 1194
resolv-retry infinite
nobind
```

Je ping l'ip du serveur vpn dans le tunnel sa passe correctement

```
# ping 10.0.0.1
*PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=3.43 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=3.51 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=3.13 ms
```

Comme on le voit ici la connexion a correctement été initialiser dans les log du serveur vpn on voit son ip dans le vlan 60 et son ip dans le tunnel qui lui a été attribuer

```
2021-11-23 08:59:23 us=411924 172.16.19.13:45657 [monclt] Peer Connection Initiated with [AF_INET]172.16.19.13:45657
2021-11-23 08:59:23 us=411939 monclt/172.16.19.13:45657 MULTI_sva: pool returned IPv4=10.0.0.6, IPv6=(Not enabled)
2021-11-23 08:59:23 us=411962 monclt/172.16.19.13:45657 MULTI: Learn: 10.0.0.6 -> monclt/172.16.19.13:45657
2021-11-23 08:59:23 us=411969 monclt/172.16.19.13:45657 MULTI: primary virtual IP for monclt/172.16.19.13:45657: 10.0.0.6
```

Je test un ping vers google avec mon interface virtuelle sur le client pour voir si le natting fonctionne correctement

C'est parfait mon vpn est maintenant configuré

```
(root@kali)~# ping 8.8.8.8 -I tun0
PING 8.8.8.8 (8.8.8.8) from 10.0.0.6 tun0: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=7.84 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=9.31 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=9.68 ms
```

Pour que tout le trafic passe directement par le vpn et que par exemple pour le ping je n'ai plus besoin de préciser tun0 mais sa passera automatiquement par le vpn je fais ceci je rajoute sa

```
push « redirect-gateway def1 »
```

Et pour le serveur DNS qu'il sois envoyer au client aussi

```
push "dhcp-option DNS 172.17.1.8"
```

```
server 10.0.0.0 255.255.255.0
push "redirect-gateway def1"
push "dhcp-option DNS 172.17.1.8"
client-to-client
```

Je redemarre le serveur et le client aussi et je teste si le DNS est bien passer d'abord je fais un traceroute du client vers google.com sans préciser d'interface pour voir si par défaut maintenant il passe par le tunnel et sa permettra de voir si le DNS est bien passé

```
# traceroute google.com
traceroute to google.com (216.58.209.238), 30 hops max, 60 byte packets
 1 10.0.0.1 (10.0.0.1) 3.550 ms 3.469 ms 3.412 ms
 2 172.19.0.2 (172.19.0.2) 3.790 ms 3.739 ms 3.682 ms
 3 172.18.0.242 (172.18.0.242) 3.904 ms 3.849 ms 3.793 ms
 4 172.16.19.254 (172.16.19.254) 4.227 ms 4.175 ms 4.123 ms
 5 * * *
 6 209.166.187.185.rev.siamko.com (185.187.166.209) 3.894 ms 3.416 ms 3.362 ms
 7 1.165.187.185.rev.siamko.com (185.187.165.1) 4.928 ms 4.890 ms 4.837 ms
 8 core-th2-gw0.levelsys.com (185.58.11.17) 4.784 ms 8.688 ms 8.649 ms
 9 xe-10-2-1.tcr2.th2.par.core.as8218.eu (83.167.39.48) 8.605 ms 8.572 ms 8.492 ms
10 google-side.tcr2.th2.par.core.as8218.eu (213.152.30.17) 9.077 ms 9.044 ms 8.996 ms
11 108.170.244.225 (108.170.244.225) 10.623 ms 10.553 ms 10.512 ms
12 108.170.238.107 (108.170.238.107) 8.799 ms 209.85.244.155 (209.85.244.155) 8.732 ms *
13 * par10s29-in-f14.1e100.net (216.58.209.238) 9.993 ms *
```

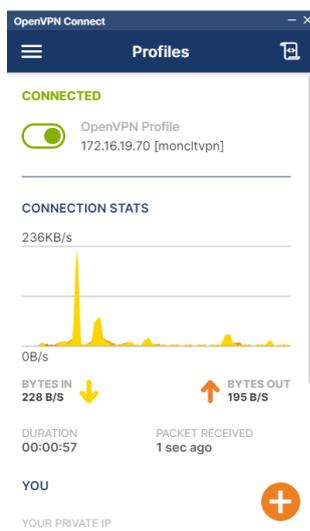
C'est bien passé ! mais pour être sûr il faut modifier le contenu de etc/resolv.conf

Sur windows j'installe le client openvpn

J'ai transféré les fichiers sur windows

Nom	Modifié le	Type	Taille
 bookticsign.key	23/11/2021 09:43	Fichier KEY	1 Ko
 ca.crt	23/11/2021 09:43	Certificat de sécur...	2 Ko
 monclt.crt	23/11/2021 09:43	Certificat de sécur...	5 Ko
 monclt.key	23/11/2021 09:43	Fichier KEY	2 Ko
 moncltvpn.ovpn	23/11/2021 09:44	OVPN Profile	1 Ko

Je me met sur le vlan 60 avec windows et me connecte sa fonctionne !



Je fais un ipconfig

```

arte inconnue Connexion au réseau local :
    Suffixe DNS propre à la connexion. . . . :
    Adresse IPv6 de liaison locale. . . . . : fe80::8d89:46d:cca3:cfdb%41
    Adresse IPv4. . . . . : 10.0.0.6
    Masque de sous-réseau. . . . . : 255.255.255.252
    Passerelle par défaut. . . . . :

```

Ping vers une machine du vlan 10

```

C:\Users\Administrateur>ping 172.17.1.8

Envoi d'une requête 'Ping' 172.17.1.8 avec 32 octets de données :
Réponse de 172.17.1.8 : octets=32 temps=3 ms TTL=126
Réponse de 172.17.1.8 : octets=32 temps=6 ms TTL=126
Réponse de 172.17.1.8 : octets=32 temps=3 ms TTL=126
Réponse de 172.17.1.8 : octets=32 temps=5 ms TTL=126

```

Tracert vers cette machine

```
C:\Users\Administrateur>tracert 172.17.1.8

Détermination de l'itinéraire vers 172.17.1.8 avec un maximum de 30 sauts.

  1      1 ms      2 ms      2 ms  10.0.0.1
  2      4 ms      3 ms      3 ms  172.19.0.2
  3      4 ms      4 ms      3 ms  172.17.1.8
```

C'est parfait

Pour une connexion via telephone voici ce qu'il faut faire

<https://www.samsufy.fr/certificat-openvpn-dans-un-seul-fichier/>

J'ai réussi à faire une connexion avec mon téléphone pour cela j'ai intégré le crt du CA le crt et key du client directement dans le fichier de conf du client et j'ai délimiter sa par des balises les voici

<ca> et </ca>

<key>

<cert>

Ensuite je colle dedans le contenu des fichiers comme ici dans les captures

```
<key>
-----BEGIN PRIVATE KEY-----
MIIEJQgIBADANBgkqhkiG9w0BAQEFAAQCCSwgggkoAgEAAoICAQC0gS6HEfLZ4SOR
m9FyDcT+r0tiwgje7FhsGNZgJT3wGnxP81N0ImEzEKUki4w70YY1Xhw9UnueKweM
8l4ELKN5eF3Xl+Qwqh4Rp0Tg35qAJPoWbSySHGEmfufusVo07ao++yV9s8w6fg3f1
VAgVrDlBT2UbSxq0X0K1i/1BD/pByx+VRf9jCi+Em3UXh8zIjE/3lDu//4rDfzc
e3I0mIwdv3g3pwPXhGLqfQ1NH9IFe3gtDXXCsCCb8MaJlvje4RJCbSvPQTW7vfqE
YGk79+tFNGp8cafa7Rh8HTYJycsvhw/00TIGIJSHKA8aFkBGcXLL2BXRXhyzgjFP
xBuoQnwB37kXQdn5H05Jiy3S9EdDcZX181IjZf00m+72AaAvm7/qI038263+S3of
fFD2TyJ+AGvsF5FP7ToXN4bmA/0jocnM3F6a3xXIIm0txY4vQnFv7t6sy/EqbFdYD
07gxVuKh4mz6ZLeVQ/RvFccFuxdeYREMAXKx5HTLFH45qSNBne57c+PLLAxauu1s
mapd1+oqIHocCNkyo5Z33DsrvHL/Y7RvRta1PapGsB8VzXI3s3hyL/X6/nmHOM36
uHqJw/07CcMsrLcaM3PVLkN5ZfVjh9XuNwpFEbzMe2dej0F5VmM4tRAXf2W8c5i1
xeZ5eLno0FgugPHrtOLDERMkjTQmIwIDA0ABAoTCAHL+ub2jWawLgpxv0QYAb7gx
xT0kkk0uUBKsm7gJm0ikn/87N4VBeaeextFLBoP6gi14A01QLWlfcv1vJ/+cgc4
/9ASHHZDYc2r14TL74okBI+1Degn3FzBdkzc8XFI+jr5361xT6e5fbr1xhDKMjg1
ln2w79M9jUg6HEa5L14vc9GQNLB7UpmE9COPsyDIb8fywocA39ReHPPH6UzEP9rL
2LLb3D65QKtS795qn0q0lnjPJC7cNmoigtLx4mRbz14yXu6zBKC078LWCTUDR0fZ
1N1jKyT2V9r6YSrrPE6BRELtBu00bg+NhdHoyxnTf0sqZwyD8JUMJI5EybwnYT9e
ZqaHXwG1/80tjlnMAm7oWSUdo80c9I/L0p7wv/T+tkkaaEhXcR5HeXVtgbVesYL3
3+gJ087hauqC9dDjQhsaaJaiTpfF/suzNRvLXuBTN8Lj/Jz0iueFNWiwMCD0UAhu
TwmVP3L6h8quHsumcFot2f6leettt5Q6PyB3F7IzScFVRfhsqSLAXNH00T5R0GRF
XwJ8eryzXR1oVUeTPJ1yw82l82MPS3g0FbVSc6/10X1ah0S50+eoBq/BEMhJJTr/
FmUipgbcGUcKHTxU3nDBRD9htJ+buTBDfr1ah/P7miEfoGKTnesGfpyMfV259R
vrl/sn86D9b0SBMKIOMBAoIBA0DcF5d6cT+Kdi+YnRvZ2N0DGOLKwJ8kA4/d4aTP
LRkVKfghVuoT038UAswDSxsaPF4ChiTUmUBbt9BCQI+5f7bwU002/WKY0NV0o3Fy
HSscjFXr040GjjPhLp9mD1Nf4eK12LxLwDiRz+pEor9MiT9y5YafSgV1W0WpkWm5
htK/0c/dvy/cLzFQR0ub0a9bvFeFaJV0oknNv422mFmZj9qDQdiEjwPhBnBaqfFD
Yw0zKPqWsaMND05D3Go3Wh9C3KpkPSdm5qDdQIR09PaFeqLz5k2e4nN8a0iqzWd
CsHompoxWT2njbaDSKRLyZsum2FgCYiyZ42niIDfw+ePFVzAoIBA0DR9Ct4skus
3s8+nWxtGznZqnaLWLkpe65yf0mGPIHoX9Uz2jbxH9FTR6q95Y0o0LEHUK4F70Az
```

```
</key>
<ca>
-----BEGIN CERTIFICATE-----
MIIFPzCCAzOgAwIBAgIUWV50X0qKjopNnHxv0qe+hmIyUzgwDQYJKoZIhvcNAQEL
B0AwFjEUBiGA1UEAwLRWzFzS1SU0EG00EWhhcnMjExMTIwMDI1OTQ1WhcNMZEx
MTE4MDI1OTQ1WjAwMRowEgYDVQODDAtFYXN5LVJlTOSBDQTCcA1IwDQYJKoZIhvcN
AQEBBQADggIPADCCAgGcggIBALCEGACKi8jqq5A5wSeVfE5WwB52E/bw6CZ+/8eT
pO/s1Z2V50zS6G0MxE03bB5c4VXRwPBW9jNrm9VJTLKsGSGokgatF2W06dORMCS
n/m06MULVD6xV9+TKrTjTs+RE5MlKUpRR00uhzjBxwELFRGq1pkVVAuB4IRT5gmUwz
Lxa0Q79Jv1uA1Nn/B1XKuc39164JS/A+XU04y1H91vMfE1w50E01Svs3h/+7SVMM
y0vq4h9PRF0Jq4Zz/nT75nU2tVLDavS4kXupqOP/ZL37PsBZydZG8AG1/6g+TWH
/EBkt4bm5SGSxUoYL1E7u7kRu+kBdqF4PtL/NAst0DCddUFBUucPhtFCKJmsvaIgb
9eunf508Xob1q0DcmQ0GZWyX58IzVDHTLSZ0UqfC+0md+TvuGEez80pKWKY0JH1
lG7d5vE1dNf0Eu1n2p/+7E0CjN2P7q99FV/ZLTSqKUM09c1ZkYXNj18Tuy8arr78
KZVKxwPc0j2E4h0L3XY0uhw500n+n0AETTVANCITEMouJc/bc6/oqBHxJjzR1M/
R2NZG1Pho0I0ohF9v5m8FF8jBjJ+Cg9RzszMuFNCArZ0r32g0FBb1Q3vmj78c+F
YYkgqkyRrhJxG0yU+YwIPwtXL6ymJ7NjctWiBBfvCggaUVdWx5DhwiFuWq+GaL9W
L77JAgMBAAGjgZAwgY0wHQYDVR00BBYEFHTLj4LX9IF5BzvmBn6TZ6qSqiMWMFEG
A1UdIWRKME1AFHTLj4LX9IF5BzvmBn6TZ6qSqiMWMORqkGDAMR0wEgYDV00DAtF
YXN5LVJlTOSBDQYlUWV50X0qKjopNnHxv0qe+hmIyUzgwDQYDVR0TBAUwAwEB/zAL
BgNVHQBAMCAQYwDQYJKoZIhvcNAQELBQADggIBABEaa3g68VatNI4Io+RkXMMU
3do1oGU1QhqbF1GxalocLwE9G3LZi1GvG+E866xxeAWRlMKnvsCRcsGKDH9fhfXI
M9FRw+LkBRp0dr1FFNkI4EUmF1XzpU8rUV2Y/adL317B1qG4dzF0IWhNnhzZ1qyF
617r10BHwZrVszf5w/v1gQSUU1Vkb20dyXDDmglZeCL05XyU/qYKL4XfIcx0Fv5
udLMZREZ8Gr8AhoGHfXrCYiSAuTAH8EUYKmXTDXtF14eCIXZVUf5wYh6C+WP7k+0
GCP+Tr+JezYcnM14DHAYUqm0g2Z2bg0F+1fM1F6TYgI+zhHVLfdgSACHAU1S0I1
HLNrp1+1b1uSo3TqYakp0sbkvteZqNA4nUN85Ag0in0blkkrieytKK6xPeXUPlf
qTlylc4n52vm0rCH0c4GdCqL6mpIFK1J6ag90+LYndUYpYZzmt0KlHlLx+MnsX1
VmGh1tY0LcWREZ+Gpc2B1SGRyPu6pk4RLhupIFdges9mVnpvwdUe0AtzjS121Rb
c4L1R9fBdwukVrPhN1nojY38zGW66Rj4ho+eV4v06aHRBz8eHZVmeLW/XdcIqqm
SMA09orgG1jMYWHA53Ev/9Ks7uqa3JxRBU/Nmk07ws1hXHuB6ARdarsfcoVRT1
Ck0m30LYLYtKyLTaF41j
-----END CERTIFICATE-----
</ca>
<cert>
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      16:f5:fa:8b:a8:be:7e:39:d3:96:b6:27:2b:3f:3a:1e
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: CN=Easy-RSA CA

```

```
ea:9c:e8:ed:bc:69:0c:00
-----BEGIN CERTIFICATE-----
MIIFVDCCAzOgAwIBAgIUQFvX6i6i+fjnTlrYnKz86HjANBgkqhkiG9w0BAQsFADQw
MRQwEgYDVQODDAtFYXN5LVJlTOSBDQTAeFw0yMTE4MDI1OTQ1WjAwMRowEgYDVQOD
DAtFYXN5LVJlTOSBDQTCcA1IwDQYJKoZIhvcNAQEBBQADggIPADCCAgGcggIBALCEG
ACKi8jqq5A5wSeVfE5WwB52E/bw6CZ+/8eTpO/s1Z2V50zS6G0MxE03bB5c4VXRw
PBW9jNrm9VJTLKsGSGokgatF2W06dORMCSn/m06MULVD6xV9+TKrTjTs+RE5MlK
UpRR00uhzjBxwELFRGq1pkVVAuB4IRT5gmUwzLxa0Q79Jv1uA1Nn/B1XKuc39164
JS/A+XU04y1H91vMfE1w50E01Svs3h/+7SVMMY0vq4h9PRF0Jq4Zz/nT75nU2tV
LDavS4kXupqOP/ZL37PsBZydZG8AG1/6g+TWH/EBkt4bm5SGSxUoYL1E7u7kRu+k
BdqF4PtL/NAst0DCddUFBUucPhtFCKJmsvaIgb9eunf508Xob1q0DcmQ0GZWyX
58IzVDHTLSZ0UqfC+0md+TvuGEez80pKWKY0JH1lG7d5vE1dNf0Eu1n2p/+7E0C
jN2P7q99FV/ZLTSqKUM09c1ZkYXNj18Tuy8arr78KZVKxwPc0j2E4h0L3XY0uhw5
00n+n0AETTVANCITEMouJc/bc6/oqBHxJjzR1M/R2NZG1Pho0I0ohF9v5m8FF8jBj
J+Cg9RzszMuFNCArZ0r32g0FBb1Q3vmj78c+FYYkgqkyRrhJxG0yU+YwIPwtXL6ym
J7NjctWiBBfvCggaUVdWx5DhwiFuWq+GaL9WL77JAgMBAAGjgZAwgY0wHQYDVR00
BBYEFHTLj4LX9IF5BzvmBn6TZ6qSqiMWMFEG A1UdIWRKME1AFHTLj4LX9IF5Bz
vmBn6TZ6qSqiMWMORqkGDAMR0wEgYDV00DAtFYXN5LVJlTOSBDQYlUWV50X0qKjop
NnHxv0qe+hmIyUzgwDQYDVR0TBAUwAwEB/zALBgNVHQBAMCAQYwDQYJKoZIhvcNA
QELBQADggIBABEaa3g68VatNI4Io+RkXMMU3do1oGU1QhqbF1GxalocLwE9G3LZi1
GvG+E866xxeAWRlMKnvsCRcsGKDH9fhfXIM9FRw+LkBRp0dr1FFNkI4EUmF1Xzp
U8rUV2Y/adL317B1qG4dzF0IWhNnhzZ1qyF617r10BHwZrVszf5w/v1gQSUU1V
kb20dyXDDmglZeCL05XyU/qYKL4XfIcx0Fv5udLMZREZ8Gr8AhoGHfXrCYiSAuTA
H8EUYKmXTDXtF14eCIXZVUf5wYh6C+WP7k+0GCP+Tr+JezYcnM14DHAYUqm0g2Z
2bg0F+1fM1F6TYgI+zhHVLfdgSACHAU1S0I1HLNrp1+1b1uSo3TqYakp0sbkvteZ
qNA4nUN85Ag0in0blkkrieytKK6xPeXUPlfqTlylc4n52vm0rCH0c4GdCqL6mpIF
K1J6ag90+LYndUYpYZzmt0KlHlLx+MnsX1VmGh1tY0LcWREZ+Gpc2B1SGRyPu6pk
4RLhupIFdges9mVnpvwdUe0AtzjS121Rbc4L1R9fBdwukVrPhN1nojY38zGW66Rj
4ho+eV4v06aHRBz8eHZVmeLW/XdcIqqmSMA09orgG1jMYWHA53Ev/9Ks7uqa3JxR
BU/Nmk07ws1hXHuB6ARdarsfcoVRT1Ck0m30LYLYtKyLTaF41j
-----END CERTIFICATE-----
</cert>

```

Je fais un test et sa fonctionne

Connexion depuis l'extérieur du lycée

Règle PAT du pare-feu pfsense :

Règles										
	Interface	Protocole	Adresse source	Ports source	Adresse de destination	Ports dest.	IP NAT	Ports NAT	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP/UDP	*	*	WAN address	1194 (OpenVPN)	172.19.0.6	1194 (OpenVPN)	Règle accès vpn maison	 

Tout ce qui vient sur l'ip du pfsense dans le WAN sur le port 1194 sera rediriger vers le port 1194 de mon serveur VPN

Une redirection de port est fait sur le pare feu en tete de réseau cronos.jjr-montmorency.org qui redirige toute les requetes sur son ip publique et port 11095 vers mon pfsense sur son port 1194 on a donc une redirection de port

Fichier de conf du client :

```
GNU nano 5.4 pcmaison.ovpn
client
dev tun
proto udp
remote cronos.jjr-montmorency.org 11095

ca ca.crt
cert pcmaison.crt
key pcmaison.key
tls-auth bookticsign.key

server 10.0.0.0 255.255.255.0
push "redirect-gateway def1"
push "dhcp-option DNS 172.17.1.8"
client-to-client
```

Ici on voit la connexion qui s'est initialisé et l'ip est mon ip publique avec ma 4G :

```
RR2021-12-01 15:35:16 us=233922 37.169.41.7:4102 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256
_GCM_SHA384, 2048 bit RSA
2021-12-01 15:35:16 us=233939 37.169.41.7:4102 [pcmaison] Peer Connection Initiated with [AF_INET]37.
169.41.7:4102
2021-12-01 15:35:16 us=233952 pcmaison/37.169.41.7:4102 MULTI_sva: pool returned IPv4=10.0.0.10, IPv6
=(Not enabled)
2021-12-01 15:35:16 us=233987 pcmaison/37.169.41.7:4102 MULTI: Learn: 10.0.0.10 -> pcmaison/37.169.41
.7:4102
2021-12-01 15:35:16 us=233994 pcmaison/37.169.41.7:4102 MULTI: primary virtual IP for pcmaison/37.169
.41.7:4102: 10.0.0.10
2021-12-01 15:35:16 us=234005 pcmaison/37.169.41.7:4102 Data Channel: using negotiated cipher 'AES-25
6-GCM'
2021-12-01 15:35:16 us=234020 pcmaison/37.169.41.7:4102 Data Channel MTU parms [ L:1550 D:1450 EF:50
EB:406 ET:0 EL:3 ]
2021-12-01 15:35:16 us=234074 pcmaison/37.169.41.7:4102 Outgoing Data Channel: Cipher 'AES-256-GCM' i
nitialized with 256 bit key
2021-12-01 15:35:16 us=234082 pcmaison/37.169.41.7:4102 Incoming Data Channel: Cipher 'AES-256-GCM' i
nitialized with 256 bit key
2021-12-01 15:35:16 us=234108 pcmaison/37.169.41.7:4102 SENT CONTROL [pcmaison]: 'PUSH_REPLY,redirect
-gateway def1,dhcp-option DNS 172.17.1.8,route 10.0.0.0 255.255.255.0,topology net30,ping 10,ping-res
tart 120,ifconfig 10.0.0.10 10.0.0.9,peer-id 0,cipher AES-256-GCM' (status=1)
R2021-12-01 15:35:16 us=234134 pcmaison/37.169.41.7:4102 PUSH: Received control message: 'PUSH_REQUES
T'
```

Sa fonctionne parfaitement la connexion est initialisé et fonctionne.

Plusieurs configuration sur le même serveur openvpn

Je crée un répertoire « seconde conf » à la racine du serveur

Ensuite j'importe le script easy-rsa dans ce répertoire et je retape la commande pour initier la pki et je crée l'autorité de certification

Ensuite je crée un certificat et une clé privée pour mon serveur et client, ici le certificat n'est pas encor signée par le CA

```
-----
Common Name (eg: your user, host, or server name) [secondeSRV]:
Keypair and certificate request completed. Your files are:
req: /secondeConf/easy-rsa/pki/reqs/secondeSRV.req
key: /secondeConf/easy-rsa/pki/private/secondeSRV.key

root@OPENVPN:/secondeConf/easy-rsa# ./easysrsa gen-req secondeCLT nopass
Using SSL: openssl OpenSSL 1.1.1k 25 Mar 2021
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/secondeConf/easy-rsa/pki/easy-rsa-26703.V6f5vb/tmp.
Kc3Phu'
-----
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.
```

Pour le signer j'utiliser cette commande /easysrsa sign-req server secondeSRV

Je crée ma clé diffie helman aussi

Fichier de conf du serveur

Je crée le fichier de conf dans /etc/openvpn/

Il s'appellera second.conf

Il ressemble à sa

```
proto udp
dev tun
port 1195
ca /secondeConf/easy-rsa/pki/ca.crt
cert /secondeConf/easy-rsa/pki/issued/secondeSRV.crt
key /secondeConf/easy-rsa/pki/private/secondeSRV.key
dh /secondeConf/easy-rsa/pki/dh.pem

server 10.1.0.0 255.255.255.0
push "redirect-gateway def1"
push "dhcp-option DNS 172.17.1.8"

client-to-client

explicit-exit-notify 1
keepalive 10 120
persist-key
persist-tun

cipher AES-256-CBC
compress lz4-v2
verb 5
```

J'ai modifié le réseau pour avoir un réseau par configuration

Bien précisé la directive port avec un port différent de notre première configuration

Un fichier de configuration par port

Ensuite je démarre ma nouvel conf comme ceci `systemctl restart openvpn@second`

Les logs :

```
root@OPENVPN:~# tail -30 /var/log/syslog
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: do_ifconfig, ip4=1, ipverb
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: net_iface_attach_mtu 1500 for tun1
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: net_iface_up: set tun1 up
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: net_addr_pton_v4 addr: 10.1.0.1 peer 10.1.0.2 dev tun1
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: net_iface_up_addr 10.1.0.0/24 via 10.1.0.2 dev [tun1] table 0 metric -1
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: Data Channel MTU parms [ L:1502 D:1450 EF:122 EB:400 ET:0 EL:0 ]
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: Could not determine IPv4/IPv6 protocol. Using AF_INET
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: Socket Buffers: R=[12292->12292] S=[12292->12292]
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: UDPv4 Link local (bound): [AF_INET][undef]:1195
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: UDPv4 Link remote: [AF_UNSPEC]
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: MULTI: multi unit called, r=256 v=256
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: IFCONFIG POOL IP4: base=10.1.0.4 size=62
Apr  8 09:34:44 OPENVPN ovpn-second[39189]: Initialization Sequence Completed
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.0570] device (tun1): state change: unmanaged -> unavailable (reason 'connection-assumed', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.0790] device (tun1): state change: unavailable -> disconnected (reason 'connection-assumed', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.0820] device (tun1): Activation: starting connection 'tun1 (57285107-6608-4802-9fa1-c8ad0222cc6c)'
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.0844] device (tun1): state change: disconnected -> prepare (reason 'none', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.0893] device (tun1): state change: prepare -> config (reason 'none', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.0910] device (tun1): state change: config -> ip-config (reason 'none', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.0986] device (tun1): state change: ip-config -> ip-check (reason 'none', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN dbus-daemon[403]: [system] Activating via systemd: service name='org.freedesktop.nm_dispatcher' unit='dbus-org.freedesktop.nm-dispatcher.service' requested by ':1.8' (uid=0 pid=404 c
/home:/usr/sbin/NetworkManager --no-daemon *)
Apr  8 09:34:44 OPENVPN systemd[1]: Starting Network Manager Script Dispatcher Service...
Apr  8 09:34:44 OPENVPN dbus-daemon[403]: [system] Successfully activated service 'org.freedesktop.nm_dispatcher'
Apr  8 09:34:44 OPENVPN systemd[1]: Started Network Manager Script Dispatcher Service.
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.1040] device (tun1): state change: ip-check -> secondaries (reason 'none', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.1061] device (tun1): state change: secondaries -> activated (reason 'none', sys-iface-state: 'external')
Apr  8 09:34:44 OPENVPN NetworkManager[404]: <info> [164903284.1090] device (tun1): Activation: successful, device activated.
Apr  8 09:34:54 OPENVPN systemd[1]: NetworkManager-dispatcher.service: Succeeded.
Apr  8 09:34:55 OPENVPN systemd[1]: Started Session 302 of user root.
Apr  8 09:34:55 OPENVPN systemd[1]: Started Session 303 of user root.
```

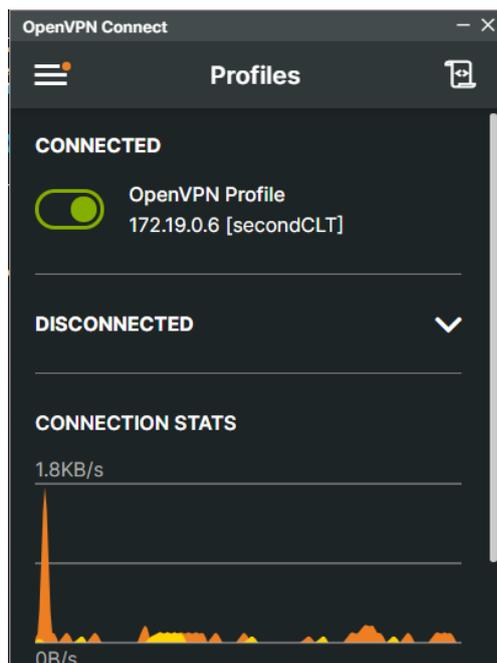
Le fichier de conf du client

```
client
dev tun
proto udp
remote 172.19.0.6 1195

ca ca.crt
cert secondeCLT.crt
key secondeCLT.key
```

Ensuite je télécharge le dossier qui contient mon fichier de conf client le certificat clé privée etc

Me voilà connecter avec mon nouveau fichier de conf



Une IP dans le réseau du nouveau fichier de conf m'a été attribuer

Je peux pinguer l'IP su serveur openvpn dans le nouveau réseau

```
08/04/2022 09:46.52 /home/mobaxterm ping 10.1.0.1
Envoi d'une requête 'Ping' 10.1.0.1 avec 32 octets de données :
Réponse de 10.1.0.1 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 10.1.0.1:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
  Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
```

Je met en place une règle de SNAT dynamique pour que les paquets sortant de ce nouveau réseau vers l'extérieur vers d'autres réseau comme le VLAN 10

iptables -t nat -A POSTROUTING -s 10.1.0.0/24 -j MASQUERADE

Je teste maintenant un ping vers un autre réseau sa passe parfaitement

```
08/04/2022 09:50.43 /home/mobaxterm ping -S 10.1.0.6 172.17.1.3
Envoi d'une requête 'Ping' 172.17.1.3 de 10.1.0.6 avec 32 octets de données :
Réponse de 172.17.1.3 : octets=32 temps=3 ms TTL=126
Réponse de 172.17.1.3 : octets=32 temps=3 ms TTL=126
Réponse de 172.17.1.3 : octets=32 temps=3 ms TTL=126
Réponse de 172.17.1.3 : octets=32 temps=2 ms TTL=126

Statistiques Ping pour 172.17.1.3:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
  Durée approximative des boucles en millisecondes :
    Minimum = 2ms, Maximum = 3ms, Moyenne = 2ms
```

Vers google :

```
08/04/2022 09:50.48 /home/mobaxterm ping -S 10.1.0.6 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 de 10.1.0.6 avec 32 octets de données :
Réponse de 8.8.8.8 : octets=32 temps=10 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=7 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=6 ms TTL=115
Réponse de 8.8.8.8 : octets=32 temps=8 ms TTL=115

Statistiques Ping pour 8.8.8.8:
  Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
  Minimum = 6ms, Maximum = 10ms, Moyenne = 7ms
```