Projet UF Infra :

Sujet réseau VPN

Thomas DUMONT

Théo DELAS

Promotion 2018/2019

B1

Dans un premier temps, lancement du serveur avec la commande « sudo openvpn server.conf » depuis le dossier « /etc/openvpn/ », ensuite lancement du client avec la commande « sudo openvpn client.conf » depuis le dossier « /etc/openvpn/ ».
Du côté du client on peut obtenir le résultat suivant :

```
[root@localhost openvpn]# openvpn client.conf
Fri Jun 28 21:02:04 2019 OpenVPN 2.4.7 x86_64-redhat-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] built on Feb 20 2019
Fri Jun 28 21:02:04 2019 library versions: OpenSSL 1.1.1c FIPS  28 May 2019, LZO 2.08
Fri Jun 28 21:02:04 2019 WARNING: No server certificate verification method has been enabled.  See http://op
envpn.net/howto.html#mitm for more info.
Enter Private Key Password: ********
Fri Jun 28 21:02:06 2019 WARNING: this configuration may cache passwords in memory -- use the auth-nocache o
ption to prevent this
Fri Jun 28 21:02:06 2019 TCP/UDP: Preserving recently used remote address: [AF_INET]92.92.168.137:2000
Fri Jun 28 21:02:06 2019 Socket Buffers: R=[212992->212992] S=[212992->212992]
Fri Jun 28 21:02:06 2019 UDP link local: (not bound)
Fri Jun 28 21:02:06 2019 UDP link remote: [AF_INET]92.92.168.137:2000
Fri Jun 28 21:02:06 2019 TLS: Initial packet from [AF_INET]92.92.168.137:2000, sid=4f4209eb dec9d7bf
Fri Jun 28 21:02:06 2019 VERIFY OK: depth=1, C=FR, ST=CA, L=Bordeaux, O=Fort-Funston, OU=MyOrganizationalUni
t, CN=ServeurVPN, name=EasyRSA, emailAddress=me@myhost.mydomain
Fri Jun 28 21:02:06 2019 VERIFY OK: depth=0, C=FR, ST=CA, L=SanFrancisco, O=Fort-Funston, OU=MyOrganizationa
lUnit, CN=serveur, name=EasyRSA, emailAddress=me@myhost.mydomain
Fri Jun 28 21:02:06 2019 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Fri Jun 28 21:02:06 2019 [serveur] Peer Connection Initiated with [AF_INET]92.92.168.137:2000
Fri Jun 28 21:02:07 2019 SENT CONTROL [serveur]: 'PUSH_REQUEST' (status=1)
Fri Jun 28 21:02:08 2019 PUSH: Received control message: 'PUSH_REPLY,redirect-gateway def1 bypass-dhcp,dhcp-
option DNS 217.237.150.188,dhcp-option DNS 8.8.8.8,route 10.8.0.0 255.255.255.0,topology net30,ifconfig 10.8
.0.6 10.8.0.5,peer-id 0,cipher AES-256-GCM'
Fri Jun 28 21:02:08 2019 OPTIONS IMPORT: --ifconfig/up options modified
Fri Jun 28 21:02:08 2019 OPTIONS IMPORT: route options modified
Fri Jun 28 21:02:08 2019 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Fri Jun 28 21:02:08 2019 OPTIONS IMPORT: peer-id set
Fri Jun 28 21:02:08 2019 OPTIONS IMPORT: adjusting link_mtu to 1625
Fri Jun 28 21:02:08 2019 OPTIONS IMPORT: data channel crypto options modified
Fri Jun 28 21:02:08 2019 Data Channel: using negotiated cipher 'AES-256-GCM'
Fri Jun 28 21:02:08 2019 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Fri Jun 28 21:02:08 2019 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Fri Jun 28 21:02:08 2019 ROUTE_GATEWAY 192.168.43.1/255.255.255.0 IFACE=wlp58s0 HWADDR=f8:59:71:94:d5:5e
Fri Jun 28 21:02:08 2019 TUN/TAP device tun0 opened
Fri Jun 28 21:02:08 2019 TUN/TAP TX queue length set to 100
Fri Jun 28 21:02:08 2019 /sbin/ip link set dev tun0 up mtu 1500
Fri Jun 28 21:02:08 2019 /sbin/ip addr add dev tun0 local 10.8.0.6 peer 10.8.0.5
Fri Jun 28 21:02:08 2019 /sbin/ip route add 92.92.168.137/32 via 192.168.43.1
Fri Jun 28 21:02:08 2019 /sbin/ip route add 0.0.0.0/1 via 10.8.0.5
Fri Jun 28 21:02:08 2019 /sbin/ip route add 128.0.0.0/1 via 10.8.0.5
Fri Jun 28 21:02:08 2019 /sbin/ip route add 10.8.0.0/24 via 10.8.0.5
Fri Jun 28 21:02:08 2019 Initialization Sequence Completed
```

La connexion au serveur fonctionne, l'ip « 92.92.168.137 » est l'adresse IP publique de la connexion internet où est connecté le serveur, qui est le Raspberry Pi.

Du côté du serveur on peut obtenir le résultat suivant en regardant les logs situés dans le fichier « /var/log/openvpn.log » :

```
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 TLS: Initial packet from [AF_INET]81.185.164.44:41685, sid=a19\
206ce bfc6dca6
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 VERIFY OK: depth=1, C=FR, ST=CA, L=Bordeaux, O=Fort-Funston, O\
U=MyOrganizationalUnit, CN=ServeurVPN, name=EasyRSA, emailAddress=me@myhost.mydomain
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 VERIFY OK: depth=0, C=US, ST=CA, L=SanFrancisco, O=Fort-Funsto\
n, OU=MyOrganizationalUnit, CN=client, name=EasyRSA, emailAddress=me@myhost.mydomain
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_VER=2.4.7
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_PLAT=linux
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_PROTO=2
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_NCP=2
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_LZ4=1
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_LZ4v2=1
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_LZO=1
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_COMP_STUB=1
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_COMP_STUBv2=1
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 peer info: IV_TCPNL=1
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 ECDHE-RSA-AES256-\
GCM-SHA384, 2048 bit RSA
Fri Jun 28 21:02:06 2019 81.185.164.44:41685 [client] Peer Connection Initiated with [AF_INET]81.185.164.44\
:41685
Fri Jun 28 21:02:06 2019 client/81.185.164.44:41685 MULTI_sva: pool returned IPv4=10.8.0.6, IPv6=(Not enabl\
ed)
Fri Jun 28 21:02:06 2019 client/81.185.164.44:41685 MULTI: Learn: 10.8.0.6 -> client/81.185.164.44:41685
Fri Jun 28 21:02:06 2019 client/81.185.164.44:41685 MULTI: primary virtual IP for client/81.185.164.44:4168\
5: 10.8.0.6
Fri Jun 28 21:02:08 2019 client/81.185.164.44:41685 PUSH: Received control message: 'PUSH_REQUEST'
Fri Jun 28 21:02:08 2019 client/81.185.164.44:41685 SENT CONTROL [client]: 'PUSH_REPLY,redirect-gateway def\
1 bypass-dhcp,dhcp-option DNS 217.237.150.188,dhcp-option DNS 8.8.8.8,route 10.8.0.0 255.255.255.0,topology\
 net30,ifconfig 10.8.0.6 10.8.0.5,peer-id 0,cipher AES-256-GCM' (status=1)
```

On peut remarquer que l'adresse IP « 81.185.164.44 », qui est l'IP publique du client, s'est bien connecté au serveur.

Grâce à la commande « traceroute » vers www.google.com, on peut confirmer que le client peut correctement accéder à internet en passant par le VPN.

```
[Akha@localhost ~]$ traceroute www.google.com
traceroute to www.google.com (172.217.18.196), 30 hops max, 60 byte packets
 1  10.8.0.1 (10.8.0.1)  58.623 ms  62.506 ms  62.462 ms
 2  192.168.1.1 (192.168.1.1)  75.548 ms  75.523 ms  93.914 ms
 3  33ton1-nro-1.nro.gaoland.net (109.24.76.20)  101.476 ms  101.376 ms  105.199 ms
 4  101.55.20.93.rev.sfr.net (93.20.55.101)  105.185 ms  105.148 ms  106.603 ms
 5  109.10.136.77.rev.sfr.net (77.136.10.109)  106.594 ms  109.623 ms  109.602 ms
 6  v3791.poi1-co-1.gaoland.net (84.96.251.165)  115.112 ms  69.818 ms  82.777 ms
 7  v3686.cae1-co-1.gaoland.net (80.118.205.129)  82.715 ms  86.648 ms  101.774 ms
 8  110.216.129.77.rev.sfr.net (77.129.216.110)  89.960 ms  86.504 ms  89.867 ms
 9  108.170.244.225 (108.170.244.225)  91.705 ms 108.170.244.161 (108.170.244.161)  99.867 ms  101.252 ms
10  66.249.94.83 (66.249.94.83)  101.283 ms 66.249.94.133 (66.249.94.133)  101.263 ms 66.249.94.83 (66.24
9.94.83)  91.817 ms
11  par10s38-in-f4.1e100.net (172.217.18.196)  91.032 ms  91.019 ms  91.582 ms
```

L'ip « 10.8.0.1 » est l'adresse IP du serveur, et l'IP « 192.168.1.1 » est celle du routeur sur lequel est connecté le Raspberry Pi.