

TP2 Accès distants - VPN

Exercice 1 :

Configurer la passerelle de sorte que le client interne ait accès à la partie internet. Il s'agira de mettre du NAT en place

Exercice 2 :

```
passerelle : 192.168.56.254/24 ;  
client-interne : 192.168.56.1/24 ;  
client-vpn: ip dynamique ;
```

Passerelle nat :

```
nano /etc/sysctl.conf  
net.ipv4.ip_forward=1  
  
iptables -t nat -A POSTROUTING -s 192.168.56.254/24 -o eth0 -j MASQUERADE
```

eth0 est l'interface de la passerelle qui donne accès à internet

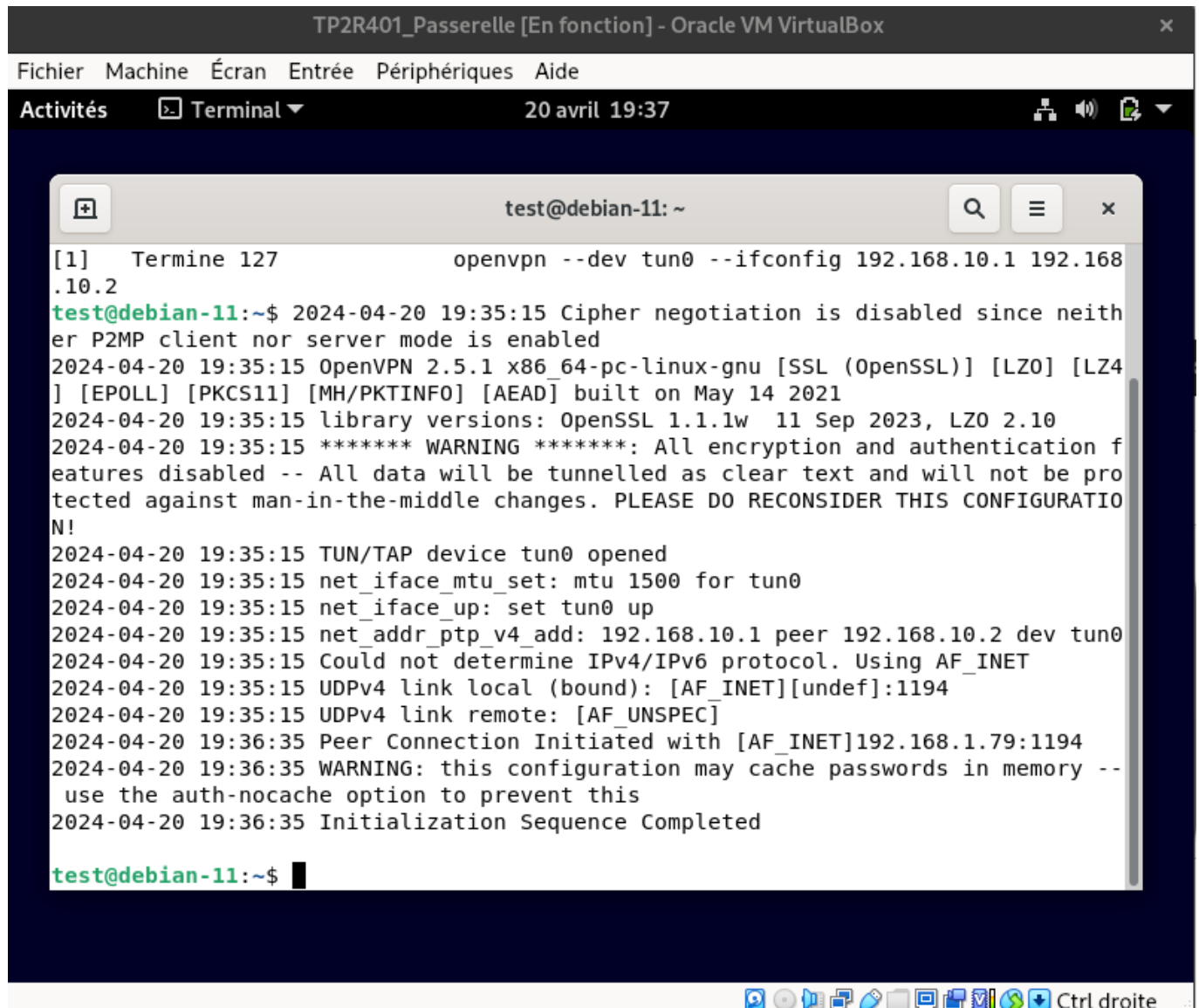
Exercice 3 :

```
apt install openvpn  
apt install liblz02-2
```

Exercice 4 :

```
passerelle :  
  
openvpn --dev tun0 --ifconfig 192.168.10.1 192.168.10.2  
  
clientVPN :  
openvpn --remote 192.168.1.79 --dev tun0 --ifconfig 192.168.10.2  
192.168.10.1
```

Exercice 5 :



```
TP2R401_Passerelle [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
Activités Terminal 20 avril 19:37

test@debian-11: ~
[1] Termine 127 openvpn --dev tun0 --ifconfig 192.168.10.1 192.168.10.2
test@debian-11:~$ 2024-04-20 19:35:15 Cipher negotiation is disabled since neither P2MP client nor server mode is enabled
2024-04-20 19:35:15 OpenVPN 2.5.1 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] built on May 14 2021
2024-04-20 19:35:15 library versions: OpenSSL 1.1.1w 11 Sep 2023, LZO 2.10
2024-04-20 19:35:15 ***** 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!
2024-04-20 19:35:15 TUN/TAP device tun0 opened
2024-04-20 19:35:15 net_iface_mtu_set: mtu 1500 for tun0
2024-04-20 19:35:15 net_iface_up: set tun0 up
2024-04-20 19:35:15 net_addr_ptp_v4_add: 192.168.10.1 peer 192.168.10.2 dev tun0
2024-04-20 19:35:15 Could not determine IPv4/IPv6 protocol. Using AF_INET
2024-04-20 19:35:15 UDPv4 link local (bound): [AF_INET][undef]:1194
2024-04-20 19:35:15 UDPv4 link remote: [AF_UNSPEC]
2024-04-20 19:36:35 Peer Connection Initiated with [AF_INET]192.168.1.79:1194
2024-04-20 19:36:35 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2024-04-20 19:36:35 Initialization Sequence Completed

test@debian-11:~$
```

on peut ping entre la machine qui a le client vpn et la passerelle. Mais pas entre la machine qui a le client vpn et la machine qui a le client interne.


Exercice 6 :

On observe la présence d'un tun0 sur les 2 machines ce qui indique donc que la connexion se fait entre c'est 2 machines par tunnel vpn.

Passerelle [En fonction] - Oracle VM VirtualBox

FichierMachineÉcranEntréePériphériquesAide

16:46:53.512091 IP debian-2.home.52244 > livebox.home.domain: 19128+ [1au] PTR? 12.1.168.192.in-addr
.arpa. (54)
16:46:53.519001 IP livebox.home.domain > debian-2.home.52244: 19128* 1/0/1 PTR redmi-note-10-pro.hom
e. (90)
^C
45 packets captured
45 packets received by filter
0 packets dropped by kernel
root@debian:~# ip -br a
lo UNKNOWN 127.0.0.1/8 ::1/128
eth0 UP 192.168.1.79/24 2a01:cb1d:8aac:8500:a00:27ff:fe40:8037/64 fe80::a00:
27ff:fe40:8037/64
eth1 UP 192.168.56.254/24
br-e7bec5ff8b73 DOWN 192.168.64.1/20
br-fcd8ede0c897 DOWN 172.26.0.1/16
br-0f628ff91cc1 DOWN 172.30.0.1/16
br-d71a2df3e4ee DOWN 172.23.0.1/16
br-c6cdd406d297 DOWN 192.168.96.1/20
br-ee41534cca6f DOWN 172.31.0.1/16
br-9b7b8d24f4ba DOWN 192.168.80.1/20
br-a90fb4de522e DOWN 172.18.0.1/16
br-3b77f34523b4 DOWN 172.19.0.1/16
br-945418f46f5d DOWN 172.24.0.1/16
br-a352deb5a7d6 DOWN 192.168.32.1/20
br-a7f4513166fd DOWN 192.168.16.1/20
br-ddd240ba385f DOWN 172.21.0.1/16
br-ec090407435b DOWN 172.27.0.1/16
br-0b8eb357c283 DOWN 172.28.0.1/16
br-25d0a337a945 DOWN 192.168.48.1/20
br-4c56485b86fc DOWN 172.20.0.1/16
br-85a4d0416957 DOWN 192.168.0.1/20
br-9b2d2ba29292 DOWN 172.25.0.1/16
br-a3b8f64625fa DOWN 172.29.0.1/16
br-15b444edc9af DOWN 172.22.0.1/16
docker0 DOWN 172.17.0.1/16
tun0 UNKNOWN 192.168.10.1 peer 192.168.10.2/32 fe80::5735:39f9:2ae2:2fca/64
root@debian:~#

 Ctrl droite

Exercice 7 :

```

Passerelle [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
r.arp. (55)
16:46:49.608724 38:b5:c9:d2:75:50 (oui Unknown) > Broadcast, ethertype Unknown (0x887b), length 60:
0x0000: 0102 0400 0487 1000 0000 0000 0000 0000 .....
0x0010: 0000 0000 0000 0000 0000 0000 0000 0000 .....
0x0020: 0000 0000 0000 0000 0000 0000 0000 0000 .....
16:46:49.611212 IP livebox.home.domain > debian-2.home.54893: 47325 NXDomain* 0/0/1 (55)
16:46:49.612378 IP debian-2.home.37345 > livebox.home.domain: 65002+ [1au] PTR? 45.1.168.192.in-addr
.arp. (54)
16:46:49.616811 IP livebox.home.domain > debian-2.home.37345: 65002* 1/0/1 PTR tizen.home. (78)
16:46:50.188263 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 84
16:46:50.188601 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 84
16:46:50.528765 ARP, Request who-has pc-19.home tell 192.168.1.254, length 46
16:46:50.558763 IP debian-2.home.48724 > livebox.home.domain: 49531+ [1au] PTR? 26.1.168.192.in-addr
.arp. (54)
16:46:50.565334 IP livebox.home.domain > debian-2.home.48724: 49531* 1/0/1 PTR pc-19.home. (78)
16:46:51.193219 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 84
16:46:51.193451 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 84
16:46:51.553378 ARP, Request who-has tizen.home tell 192.168.1.254, length 46
16:46:52.194590 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 84
16:46:52.194780 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 84
16:46:52.510805 ARP, Request who-has livebox.home tell debian-2.home, length 28
16:46:52.517455 ARP, Reply livebox.home is-at 38:b5:c9:d2:75:50 (oui Unknown), length 46
16:46:52.580298 IP livebox.home.bootps > 255.255.255.255.bootpc: BOOTP/DHCP, Reply, length 339
16:46:53.197126 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 84
16:46:53.197348 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 84
16:46:53.258862 ARP, Request who-has debian-2.home tell debian-3.home, length 46
16:46:53.258885 ARP, Reply debian-2.home is-at 08:00:27:40:80:37 (oui Unknown), length 28
16:46:53.500027 ARP, Request who-has redmi-note-10-pro.home tell 192.168.1.254, length 46
16:46:53.512091 IP debian-2.home.52244 > livebox.home.domain: 19128+ [1au] PTR? 12.1.168.192.in-addr
.arp. (54)
16:46:53.519001 IP livebox.home.domain > debian-2.home.52244: 19128* 1/0/1 PTR redmi-note-10-pro.hom
e. (90)
^C
45 packets captured
45 packets received by filter
0 packets dropped by kernel
root@debian:~# _

```

On peut voir que les trames openvpn sont transmises en UDP.

PS : j'ai utilisé tcpdump pour voir les trames openvpn, étant donné que le groupe wireshark n'était pas associé à mon utilisateur qui a les rôles root.

Exercice 8 :

```

Passerelle [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
17:13:06.242103 IP debian-2.home.57860 > 194.199.227.220.https: Flags [..], ack 3727, win 490, option
s [nop,nop,TS val 3802515274 ecr 2385506927], length 0
17:13:06.243123 IP debian-2.home.57860 > 194.199.227.220.https: Flags [P..], seq 255:348, ack 3727, w
in 501, options [nop,nop,TS val 3802515275 ecr 2385506927], length 93
17:13:06.276013 IP 194.199.227.220.https > debian-2.home.57860: Flags [P..], seq 3727:3778, ack 348,
win 85, options [nop,nop,TS val 2385506962 ecr 3802515275], length 51
17:13:06.276727 IP debian-2.home.57860 > 194.199.227.220.https: Flags [P..], seq 348:1556, ack 3778,
win 501, options [nop,nop,TS val 3802515309 ecr 2385506962], length 1208
17:13:06.277133 IP debian-2.home.57860 > 194.199.227.220.https: Flags [P..], seq 1556:1799, ack 3778,
win 501, options [nop,nop,TS val 3802515309 ecr 2385506962], length 243
17:13:06.317310 IP 194.199.227.220.https > debian-2.home.57860: Flags [..], ack 1799, win 83, options
[nop,nop,TS val 2385506995 ecr 3802515309], length 0
17:13:06.317310 IP 194.199.227.220.https > debian-2.home.57860: Flags [P..], seq 3778:4211, ack 1799,
win 83, options [nop,nop,TS val 2385507000 ecr 3802515309], length 433
17:13:06.317310 IP 194.199.227.220.https > debian-2.home.57860: Flags [P..], seq 4211:4242, ack 1799,
win 83, options [nop,nop,TS val 2385507000 ecr 3802515309], length 31
17:13:06.317310 IP 194.199.227.220.https > debian-2.home.57860: Flags [F..], seq 4242, ack 1799, win
83, options [nop,nop,TS val 2385507000 ecr 3802515309], length 0
17:13:06.317503 IP debian-2.home.57860 > 194.199.227.220.https: Flags [..], ack 4243, win 501, option
s [nop,nop,TS val 3802515349 ecr 2385507000], length 0
17:13:06.317601 IP debian-2.home.57860 > 194.199.227.220.https: Flags [P..], seq 1799:1830, ack 4243,
win 501, options [nop,nop,TS val 3802515349 ecr 2385507000], length 31
17:13:06.317724 IP debian-2.home.57860 > 194.199.227.220.https: Flags [F..], seq 1830, ack 4243, win
501, options [nop,nop,TS val 3802515350 ecr 2385507000], length 0
17:13:06.353752 IP 194.199.227.220.https > debian-2.home.57860: Flags [R..], seq 1479728220, win 0, le
ngth 0
17:13:06.353752 IP 194.199.227.220.https > debian-2.home.57860: Flags [R..], seq 1479728220, win 0, le
ngth 0
17:13:08.094462 IP livebox.home > all-systems.mcast.net: igmp query v2
17:13:08.163379 IP6 debian.36159 > livebox.home.domain: 36528+ [1au] PTR? 1.0.0.224.in-addr.arpa. (5
1)
17:13:08.188578 IP6 livebox.home.domain > debian.36159: 36528 1/0/1 PTR all-systems.mcast.net. (86)
^C
307 packets captured
307 packets received by filter
0 packets dropped by kernel
root@debian:~#

```

On peut voir ici que chaque touche tapée sur le client vpn est transmise à la passerelle.

Exercice 9 :

On va generer notre clef partagée avec la commande suivante :

```
openvpn --genkey --secret static.key
```

Le fichier static.key contient la clef générée.

Exercice 10 : De quel type de clé s'agit-il ?

Il s'agit d'une clé symétrique.

Exercice 11 :

Sa longueur est de 2048 bits.

Exercice 12 :

Il faut maintenant transférer cette clé de façon sécurisée sur le client. Comment procéder ?

On peut utiliser la commande scp pour transférer la clé de la passerelle vers le client.

```
scp static.key root@192.168.1.80:/chemin/vers/votre/clef
```

Relancez le VPN entre les deux machines en concaténant aux commandes précédentes la directive suivante :

```
--secret /chemin/vers/votre/clef
```

Donc :

```
openvpn --dev tun0 --ifconfig 192.168.10.1 192.168.10.2 --secret static.key  
  
openvpn --remote 192.168.1.79 --dev tun0 --ifconfig 192.168.10.2  
192.168.10.1 --secret static.key
```

Exercice 13 :

```

Passerelle [En fonction] - Oracle VM VirtualBox
Fichier  Machine  Écran  Entrée  Périphériques  Aide
05, length 32
17:34:44.533599 IP6 _gateway > ff02::1: ICMP6, neighbor solicitation, who has fe80::bf55:c6e8:5a39:3
364, length 32
17:34:44.533600 IP6 _gateway > ff02::1: ICMP6, neighbor solicitation, who has debian, length 32
17:34:44.533600 IP6 _gateway > ff02::1: ICMP6, neighbor solicitation, who has fe80::a00:27ff:fe60:2f
94, length 32
17:34:44.533600 IP6 _gateway > ff02::1: ICMP6, neighbor solicitation, who has 2a01:cb1d:8aac:8500:4d
b4:f760:8c48:a65f, length 32
17:34:44.533600 IP6 _gateway > ff02::1: ICMP6, neighbor solicitation, who has 2a01:cb1d:8aac:8500:b0
19:aa28:2f4d:540b, length 32
17:34:44.533763 IP6 debian > _gateway: ICMP6, neighbor advertisement, tgt is debian, length 32
17:34:44.590902 IP debian-2.home.41259 > livebox.home.domain: 48176+ [1au] PTR? f.5.6.a.8.4.c.8.0.6.
7.f.4.b.d.4.0.0.5.8.c.a.a.8.d.1.b.c.1.0.a.2.ip6.arpa. (101)
17:34:44.634047 IP livebox.home.domain > debian-2.home.41259: 48176 NXDomain 0/1/1 (201)
17:34:45.347951 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 124
17:34:45.348442 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 124
17:34:45.964838 ARP, Request who-has envoy.home tell 192.168.1.254, length 46
17:34:46.353667 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 124
17:34:46.354001 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 124
17:34:46.989598 ARP, Request who-has s22mehdidonc.home tell 192.168.1.254, length 46
17:34:47.353252 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 124
17:34:47.353929 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 124
17:34:48.016928 ARP, Request who-has brw541379264bb8.home tell 192.168.1.254, length 46
17:34:48.355034 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 124
17:34:48.355601 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 124
17:34:48.936982 ARP, Request who-has desktop-2vgq177.home tell 192.168.1.254, length 46
17:34:49.357456 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 124
17:34:49.357969 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 124
17:34:49.961331 ARP, Request who-has fivemdev.home tell 192.168.1.254, length 46
17:34:50.063276 ARP, Request who-has livebox.home tell 192.168.1.254, length 46
17:34:50.359485 IP debian-3.home.openvpn > debian-2.home.openvpn: UDP, length 124
17:34:50.360056 IP debian-2.home.openvpn > debian-3.home.openvpn: UDP, length 124
^C
237 packets captured
237 packets received by filter
0 packets dropped by kernel
root@debian:~# _
Ctrl droite

```

On peut voir une longueur de 128 bits pour les trames openvpn. Contrairement auparavant où les trames étaient à 84 bits de longueur pour les mêmes demandes (ping).

Ce qui indique que les trames sont chiffrées.

Exercice 14 : Pour gagner de la bande passante on ajoute la directive suivante :

```
--comp-lzo --keepalive 10 60 --float
```

Exercice 15 :

Explication :

l'option `--comp-lzo` permet de compresser les données transmises, ce qui permet de gagner de la bande passante.

l'option `--keepalive` permet de garder la connexion active en envoyant un paquet toutes les 10 secondes.

le 60 est le nombre de secondes avant de considérer la connexion comme perdue.

l'option `--float` permet de permettre au client de changer d'adresse IP sans avoir à se reconnecter.

Pour simplifier la connexion il est préférable de créer un fichier de configuration pour le client d'abord

```
nano client.conf
dev tun0
remote 192.168.1.79
ifconfig 192.168.10.2 192.168.10.1
secret static.key
comp-lzo
keepalive 10 60
float
```

Ensuite on peut lancer la connexion avec la commande suivante :

```
openvpn client.conf
```

Exercice 16 :

On fait la meme chose pour le serveur :

```
nano serveur.conf
dev tun0
ifconfig 192.168.10.1 192.168.10.2
secret static.key
comp-lzo
keepalive 10 60
float
```

Ensuite on peut lancer la connexion avec la commande suivante :

```
openvpn serveur.conf
```



```

ClientVPN [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
2024-04-21 17:51:07 library versions: OpenSSL 1.1.1n 15 Mar 2022, LZ4 2.10
2024-04-21 17:51:07 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.
2024-04-21 17:51:07 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.
2024-04-21 17:51:07 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.
2024-04-21 17:51:07 TUN/TAP device tun0 opened
2024-04-21 17:51:07 net_iface_mtu_set: mtu 1500 for tun0
2024-04-21 17:51:07 net_iface_up: set tun0 up
2024-04-21 17:51:07 net_addr_pton_v4_add: 192.168.10.2 peer 192.168.10.1 dev tun0
2024-04-21 17:51:07 TCP/UDP: Preserving recently used remote address: [AF_INET]192.168.1.79:1194
2024-04-21 17:51:07 UDP link local (bound): [AF_INET][undef]:1194
2024-04-21 17:51:07 UDP link remote: [AF_INET]192.168.1.79:1194

root@debian:~# 2024-04-21 17:51:11 Peer Connection Initiated with [AF_INET]192.168.1.79:1194
2024-04-21 17:51:12 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2024-04-21 17:51:12 Initialization Sequence Completed

root@debian:~#
root@debian:~# ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=64 time=0.872 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=64 time=2.63 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=64 time=0.977 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=64 time=1.54 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=64 time=1.96 ms
^C
--- 192.168.10.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5015ms
rtt min/avg/max/mdev = 0.872/1.504/2.628/0.625 ms
root@debian:~# _

```

Exercice 17 :

Le TLS est un protocole de sécurisation des échanges sur internet. Il permet de chiffrer les données transmises entre le client et le serveur.

PS : J'ai pu de mon côté mettre en place sur le principe de public key infrastructure un VPN en utilisant wireguard.