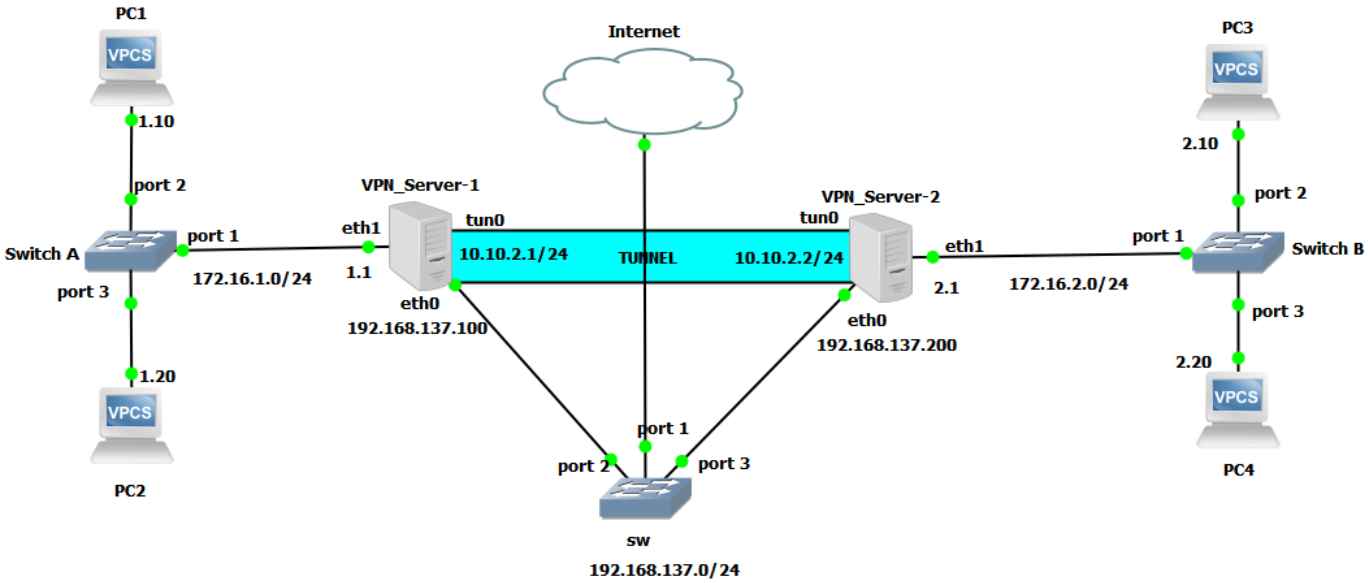
# Fiche TP N° 2 : Réseaux Privés Virtuels (VPN)

## Solution

***Partie 1 : VPN site-à-site avec GRE***

Nous considérons le schéma réseau d'une entreprise avec deux sites reliés par un tunnel VPN représenté ci-dessous.




**Remarque :**

Le login et mot de passe pour les serveurs VPN sont :
Login : user
Password : user

a) Câbler le schéma réseau ci-dessus. Ensuite, configurez les passerelles (interfaces, routage, NAT) et les clients (interface) dans chaque réseau de l'entreprise.

PC 1 :
***ip 172.16.1.10/24 172.16.1.1***
***save pc1.vpc***

PC 2 :
***ip 172.16.1.20/24 172.16.1.1***
***save pc2.vpc***

PC 3 :
***ip 172.16.2.10/24 172.16.2.1***
***save pc3.vpc***

PC 4 :
***ip 172.16.2.20/24 172.16.2.1***
***save pc4.vpc***

VPN_Server_1 :

***sudo ip addr add 192.168.137.100/24 dev eth0***
***sudo ip link set dev eth0 up***
***sudo ip addr add 172.16.1.1/24 dev eth1***
***sudo ip link set dev eth1 up***
***sudo ip route add default via 192.168.137.1 dev eth0***
***sudo ip route add 172.16.2.0/24 via 192.168.137.1 dev eth0***
***sudo sysctl -w net.ipv4.ip_forward=1***
***sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE***

```
user@ubuntu:~$ sudo ip addr add 192.168.137.100/24 dev eth0
[sudo] password for user:
user@ubuntu:~$ sudo ip link set dev eth0 up
user@ubuntu:~$ sudo ip addr add 172.16.1.1/24 dev eth1
user@ubuntu:~$ sudo ip link set dev eth1 up
user@ubuntu:~$ sudo ip route add default via 192.168.137.1 dev eth0
user@ubuntu:~$ sudo ip route add 172.16.2.0/24 via 192.168.137.1 dev eth0
user@ubuntu:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
user@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

VPN_Server_2 :

***sudo ip addr add 192.168.137.200/24 dev eth0***
***sudo ip link set dev eth0 up***
***sudo ip addr add 172.16.2.1/24 dev eth1***
***sudo ip link set dev eth1 up***
***sudo ip route add default via 192.168.137.1 dev eth0***
***sudo ip route add 172.16.1.0/24 via 192.168.137.1 dev eth0***
***sudo sysctl -w net.ipv4.ip_forward=1***
***sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE***

```
user@ubuntu:~$ sudo ip addr add 192.168.137.200/24 dev eth0
[sudo] password for user:
user@ubuntu:~$ sudo ip link set dev eth0 up
user@ubuntu:~$ sudo ip addr add 172.16.2.1/24 dev eth1
user@ubuntu:~$ sudo ip link set dev eth1 up
user@ubuntu:~$ sudo ip route add default via 192.168.137.1 dev eth0
user@ubuntu:~$ sudo ip route add 172.16.1.0 via 192.168.137.1 dev eth0
user@ubuntu:~$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
user@ubuntu:~$ sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

DANS votre Système d'exploitation :

1. Pour Windows (A partir du CMD en mode administrateur):

***route add 172.16.1.0 mask 255.255.255.0 192.168.137.100 METRIC 1***
***route add 172.16.2.0 mask 255.255.255.0 192.168.137.200 METRIC 1***

```
C:\WINDOWS\system32>route add 172.16.1.0 mask 255.255.255.0 192.168.137.100 METRIC 1
 OK!

C:\WINDOWS\system32>route add 172.16.2.0 mask 255.255.255.0 192.168.137.200 METRIC 1
 OK!
```

2. Pour Ubuntu ( A partir du Terminal) :

***sudo ip route add 172.16.1.0/24 via 192.168.137.100 dev INTERFACE*** (INTERFACE : correspond à l'interface de connexion du réseau 192.168.137.1)

***sudo ip route add 172.16.2.0/24 via 192.168.137.200 dev INTERFACE***

Valider le fonctionnement du réseau à l'aide de commandes de diagnostic (ping).

A partir du VPN_Server_1 :

***Connectivité avec le réseau 172.16.1.0/24 :***

***ping -c 4 172.16.1.10***

***ping -c 4 172.16.1.20***

```
user@ubuntu:~$ ping -c 4 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
64 bytes from 172.16.1.10: icmp_seq=1 ttl=64 time=1.62 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=64 time=2.04 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=64 time=1.75 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=64 time=1.78 ms

--- 172.16.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.627/1.801/2.042/0.156 ms
user@ubuntu:~$ ping -c 4 172.16.1.20
PING 172.16.1.20 (172.16.1.20) 56(84) bytes of data.
64 bytes from 172.16.1.20: icmp_seq=1 ttl=64 time=2.15 ms
64 bytes from 172.16.1.20: icmp_seq=2 ttl=64 time=1.59 ms
64 bytes from 172.16.1.20: icmp_seq=3 ttl=64 time=1.78 ms
64 bytes from 172.16.1.20: icmp_seq=4 ttl=64 time=0.696 ms

--- 172.16.1.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.696/1.558/2.154/0.538 ms
```

***Connectivité avec le réseau 192.168.137.0/24 :***

***ping -c 4 192.168.137.1***

***ping -c 4 192.168.137.200***

```
user@ubuntu:~$ ping -c 4 192.168.137.1
PING 192.168.137.1 (192.168.137.1) 56(84) bytes of data.
64 bytes from 192.168.137.1: icmp_seq=1 ttl=128 time=1.16 ms
64 bytes from 192.168.137.1: icmp_seq=2 ttl=128 time=1.92 ms
64 bytes from 192.168.137.1: icmp_seq=3 ttl=128 time=1.92 ms
64 bytes from 192.168.137.1: icmp_seq=4 ttl=128 time=1.89 ms

--- 192.168.137.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.164/1.725/1.921/0.324 ms
user@ubuntu:~$ ping -c 4 192.168.137.200
PING 192.168.137.200 (192.168.137.200) 56(84) bytes of data.
64 bytes from 192.168.137.200: icmp_seq=1 ttl=64 time=0.966 ms
64 bytes from 192.168.137.200: icmp_seq=2 ttl=64 time=0.730 ms
64 bytes from 192.168.137.200: icmp_seq=3 ttl=64 time=1.92 ms
64 bytes from 192.168.137.200: icmp_seq=4 ttl=64 time=2.06 ms

--- 192.168.137.200 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.730/1.421/2.065/0.583 ms
```

***Connectivité avec l'Internet :***

***ping -c 4 8.8.8.8***

```
user@ubuntu:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=43 time=71.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=43 time=70.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=43 time=70.9 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=43 time=69.5 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 69.567/70.591/71.044/0.655 ms
```

***Connectivité avec le réseau 172.16.2.0/24 :***

***ping -c 4 172.16.2.1***

***ping -c 4 172.16.2.10***

***ping -c 4 172.16.2.20***

```
user@ubuntu:~$ ping -c 4 172.16.2.1
PING 172.16.2.1 (172.16.2.1) 56(84) bytes of data.
From 192.168.137.1: icmp_seq=1 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.1: icmp_seq=1 ttl=64 time=1.52 ms
From 192.168.137.1: icmp_seq=2 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.1: icmp_seq=2 ttl=64 time=1.55 ms
From 192.168.137.1: icmp_seq=3 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.1: icmp_seq=3 ttl=64 time=2.94 ms
From 192.168.137.1: icmp_seq=4 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.1: icmp_seq=4 ttl=64 time=3.12 ms

--- 172.16.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.523/2.286/3.125/0.751 ms
```

```
user@ubuntu:~$ ping -c 4 172.16.2.10
PING 172.16.2.10 (172.16.2.10) 56(84) bytes of data.
From 192.168.137.1: icmp_seq=1 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.10: icmp_seq=1 ttl=63 time=4.60 ms
From 192.168.137.1: icmp_seq=2 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.10: icmp_seq=2 ttl=63 time=5.97 ms
From 192.168.137.1: icmp_seq=3 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.10: icmp_seq=3 ttl=63 time=1.85 ms
From 192.168.137.1: icmp_seq=4 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.10: icmp_seq=4 ttl=63 time=4.97 ms

--- 172.16.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.859/4.352/5.976/1.526 ms
```

```
user@ubuntu:~$ ping -c 4 172.16.2.20
PING 172.16.2.20 (172.16.2.20) 56(84) bytes of data.
From 192.168.137.1: icmp_seq=1 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.20: icmp_seq=1 ttl=63 time=2.88 ms
From 192.168.137.1: icmp_seq=2 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.20: icmp_seq=2 ttl=63 time=2.55 ms
From 192.168.137.1: icmp_seq=3 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.20: icmp_seq=3 ttl=63 time=2.58 ms
From 192.168.137.1: icmp_seq=4 Redirect Network(New nexthop: 192.168.137.200)
64 bytes from 172.16.2.20: icmp_seq=4 ttl=63 time=2.81 ms

--- 172.16.2.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.559/2.709/2.889/0.156 ms
```

A partir du VPN_Server_2 :

***Connectivité avec le réseau 172.16.2.0/24 :***

***ping -c 4 172.16.2.10***

***ping -c 4 172.16.2.20***

```
user@ubuntu:~$ ping -c 4 172.16.2.10
PING 172.16.2.10 (172.16.2.10) 56(84) bytes of data.
64 bytes from 172.16.2.10: icmp_seq=1 ttl=64 time=1.57 ms
64 bytes from 172.16.2.10: icmp_seq=2 ttl=64 time=2.08 ms
64 bytes from 172.16.2.10: icmp_seq=3 ttl=64 time=1.46 ms
64 bytes from 172.16.2.10: icmp_seq=4 ttl=64 time=1.64 ms

--- 172.16.2.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 1.461/1.688/2.080/0.240 ms
user@ubuntu:~$ ping -c 4 172.16.2.20
PING 172.16.2.20 (172.16.2.20) 56(84) bytes of data.
64 bytes from 172.16.2.20: icmp_seq=1 ttl=64 time=1.81 ms
64 bytes from 172.16.2.20: icmp_seq=2 ttl=64 time=1.11 ms
64 bytes from 172.16.2.20: icmp_seq=3 ttl=64 time=0.519 ms
64 bytes from 172.16.2.20: icmp_seq=4 ttl=64 time=1.01 ms

--- 172.16.2.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.519/1.113/1.811/0.462 ms
```

***Connectivité avec le réseau 192.168.137.0/24 :***

***ping -c 4 192.168.137.1***

***ping -c 4 192.168.137.100***

```
user@ubuntu:~$ ping -c 4 192.168.137.1
PING 192.168.137.1 (192.168.137.1) 56(84) bytes of data.
64 bytes from 192.168.137.1: icmp_seq=1 ttl=128 time=0.996 ms
64 bytes from 192.168.137.1: icmp_seq=2 ttl=128 time=0.682 ms
64 bytes from 192.168.137.1: icmp_seq=3 ttl=128 time=0.943 ms
64 bytes from 192.168.137.1: icmp_seq=4 ttl=128 time=0.944 ms

--- 192.168.137.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.682/0.891/0.996/0.124 ms
user@ubuntu:~$ ping -c 4 192.168.137.100
PING 192.168.137.100 (192.168.137.100) 56(84) bytes of data.
64 bytes from 192.168.137.100: icmp_seq=1 ttl=64 time=0.916 ms
64 bytes from 192.168.137.100: icmp_seq=2 ttl=64 time=0.936 ms
64 bytes from 192.168.137.100: icmp_seq=3 ttl=64 time=0.899 ms
64 bytes from 192.168.137.100: icmp_seq=4 ttl=64 time=0.928 ms

--- 192.168.137.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 0.899/0.919/0.936/0.039 ms
```

***Connectivité avec l'Internet:***

***ping -c 4 8.8.8.8***

```
user@ubuntu:~$ ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=43 time=148 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=43 time=72.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=43 time=70.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=43 time=69.9 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 69.955/90.455/148.542/33.557 ms
```

***Connectivité avec le réseau 172.16.1.0/24 :***

***ping -c 4 172.16.1.1***

***ping -c 4 172.16.1.10***

***ping -c 4 172.16.1.20***

```
user@ubuntu:~$ ping -c 4 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
From 192.168.137.1: icmp_seq=1 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.1: icmp_seq=1 ttl=64 time=2.25 ms
From 192.168.137.1: icmp_seq=2 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.1: icmp_seq=2 ttl=64 time=1.61 ms
From 192.168.137.1: icmp_seq=3 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.1: icmp_seq=3 ttl=64 time=8.87 ms
From 192.168.137.1: icmp_seq=4 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.1: icmp_seq=4 ttl=64 time=1.13 ms

--- 172.16.1.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 1.136/3.470/8.872/3.144 ms
```

```
user@ubuntu:~$ ping -c 4 172.16.1.10
PING 172.16.1.10 (172.16.1.10) 56(84) bytes of data.
From 192.168.137.1: icmp_seq=1 Redirect Network(New nexthop: 192.168.137.100)
From 192.168.137.1: icmp_seq=2 Redirect Network(New nexthop: 192.168.137.100)
From 192.168.137.1: icmp_seq=3 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.10: icmp_seq=1 ttl=63 time=3006 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=63 time=2004 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=63 time=1002 ms
From 192.168.137.1: icmp_seq=4 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.10: icmp_seq=4 ttl=63 time=2.05 ms

--- 172.16.1.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 2.058/1503.933/3006.803/1119.867 ms, pipe 4
```

```
user@ubuntu:~$ ping -c 4 172.16.1.20
PING 172.16.1.20 (172.16.1.20) 56(84) bytes of data.
From 192.168.137.1: icmp_seq=1 Redirect Network(New nexthop: 192.168.137.100)
From 192.168.137.1: icmp_seq=2 Redirect Network(New nexthop: 192.168.137.100)
From 192.168.137.1: icmp_seq=3 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.20: icmp_seq=1 ttl=63 time=3004 ms
64 bytes from 172.16.1.20: icmp_seq=2 ttl=63 time=2002 ms
64 bytes from 172.16.1.20: icmp_seq=3 ttl=63 time=1000 ms
From 192.168.137.1: icmp_seq=4 Redirect Network(New nexthop: 192.168.137.100)
64 bytes from 172.16.1.20: icmp_seq=4 ttl=63 time=2.31 ms

--- 172.16.1.20 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 2.314/1502.307/3004.001/1118.822 ms, pipe 3
```

A partir du PC 1 vers le PC 3:

PC1

```
VPCS-1> ping 172.16.2.10
84 bytes from 172.16.2.10 icmp_seq=1 ttl=62 time=2.879 ms
84 bytes from 172.16.2.10 icmp_seq=2 ttl=62 time=2.878 ms
84 bytes from 172.16.2.10 icmp_seq=3 ttl=62 time=2.896 ms
84 bytes from 172.16.2.10 icmp_seq=4 ttl=62 time=2.882 ms
84 bytes from 172.16.2.10 icmp_seq=5 ttl=62 time=0.968 ms
```

A partir du PC 4 vers le PC 2:

PC4

```
VPCS-4> ping 172.16.1.20
84 bytes from 172.16.1.20 icmp_seq=1 ttl=62 time=2.881 ms
84 bytes from 172.16.1.20 icmp_seq=2 ttl=62 time=4.889 ms
84 bytes from 172.16.1.20 icmp_seq=3 ttl=62 time=5.812 ms
84 bytes from 172.16.1.20 icmp_seq=4 ttl=62 time=2.903 ms
84 bytes from 172.16.1.20 icmp_seq=5 ttl=62 time=2.967 ms
```

**Remarque :**

- Si vous n'arrivez pas à avoir une connectivité essayez de désactiver votre pare-feu et de vérifier les routes sur votre machine hôte (Windows : ***route print,*** Ubuntu : ***ip route***).

b) Configurer un tunnel GRE entre les deux sites de l'entreprise.

VPN_Server_1 :

***sudo ip tunnel add tun0 mode gre remote 192.168.137.200 local 192.168.137.100***
***sudo ip link set dev tun0 up***
***sudo ip addr add 10.10.2.1/24 dev tun0***

```
user@ubuntu:~$ sudo ip tunnel add tun0 mode gre remote 192.168.137.200 local 192.168.137.100
user@ubuntu:~$ sudo ip link set dev tun0 up
user@ubuntu:~$ sudo ip addr add 10.10.2.1/24 dev tun0
```

VPN_Server_2 :

***sudo ip tunnel add tun0 mode gre remote 192.168.137.100 local 192.168.137.200***
***sudo ip link set dev tun0 up***
***sudo ip addr add 10.10.2.2/24 dev tun0***

```
user@ubuntu:~$ sudo ip tunnel add tun0 mode gre remote 192.168.137.100 local 192.168.137.200
user@ubuntu:~$ sudo ip link set dev tun0 up
user@ubuntu:~$ sudo ip addr add 10.10.2.2/24 dev tun0
```

Valider le fonctionnement du tunnel à l'aide de commandes de diagnostique (affichage des adresses des interfaces, tables de routage, connexion client-à-client du tunnel).

A partir du VPN_SERVER_1 vers VPN_SERVER_2:

```
user@ubuntu:~$ ping -c 4 10.10.2.2
PING 10.10.2.2 (10.10.2.2) 56(84) bytes of data.
64 bytes from 10.10.2.2: icmp_seq=1 ttl=64 time=0.994 ms
64 bytes from 10.10.2.2: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 10.10.2.2: icmp_seq=3 ttl=64 time=1.12 ms
64 bytes from 10.10.2.2: icmp_seq=4 ttl=64 time=1.02 ms

--- 10.10.2.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.994/1.047/1.128/0.059 ms
```

A partir du VPN_SERVER_1 vers VPN_SERVER_2:

```
user@ubuntu:~$ ping -c 4 10.10.2.1
PING 10.10.2.1 (10.10.2.1) 56(84) bytes of data.
64 bytes from 10.10.2.1: icmp_seq=1 ttl=64 time=1.05 ms
64 bytes from 10.10.2.1: icmp_seq=2 ttl=64 time=1.00 ms
64 bytes from 10.10.2.1: icmp_seq=3 ttl=64 time=1.19 ms
64 bytes from 10.10.2.1: icmp_seq=4 ttl=64 time=1.07 ms

--- 10.10.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 1.000/1.080/1.191/0.080 ms
```

c) Quelle est la valeur de la MTU dans le tunnel ? Expliquer le résultat.

```
user@ubuntu:~$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 08:00:27:28:f3:51 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.100/24 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe28:f351/64 scope link
       valid_lft forever preferred_lft forever
user@ubuntu:~$ ip addr show tun0
15: tun0@NONE: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1476 qdisc noqueue state UNKNOWN group default ql
en 1
    link/gre 192.168.137.100 peer 192.168.137.200
    inet 10.10.2.1/24 scope global tun0
       valid_lft forever preferred_lft forever
    inet6 fe80::5efe:c0a8:8964/64 scope link
       valid_lft forever preferred_lft forever
```

MTU (Maximum Transmission Unit) : correspond à la taille de la plus grande unité de données de protocole de couche réseau qui peut être communiquée dans une seule transaction de réseau. Dans le cas de TCP/IP avec ETHERNET cette valeur est égale à 1500 octets (comme le montre le figure de l'affichage de l'interface eth0)

Dans le cas tu tunnel, la valeur du MTU est 1476 octets.

1500 – 24 = 1476 (les 24 octets correspondent à l'entête du protocole GRE qui va encapsuler la paquet ip).

d) Démarrer une capture de trafic réseau dans VPN_server_1 avec la commande :
***tcpdump -vi eth0 proto gre***
Ensuite lancer un ping à partir de VPN_Server_2 pour le VPN_Server_1:
***ping 10.10.2.1***

```
user@ubuntu:~$ sudo tcpdump -vi eth0 proto gre
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:14:17.206054 IP (tos 0x0, ttl 64, id 60149, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.200 > 192.168.137.100: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 28710, offset 0, flags [DF], proto ICMP (1), length 84)
    10.10.2.2 > 10.10.2.1: ICMP echo request, id 1680, seq 1, length 64
20:14:17.206154 IP (tos 0x0, ttl 64, id 3683, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.100 > 192.168.137.200: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 11601, offset 0, flags [none], proto ICMP (1), length 84)
    10.10.2.1 > 10.10.2.2: ICMP echo reply, id 1680, seq 1, length 64
20:14:18.207899 IP (tos 0x0, ttl 64, id 60162, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.200 > 192.168.137.100: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 28818, offset 0, flags [DF], proto ICMP (1), length 84)
    10.10.2.2 > 10.10.2.1: ICMP echo request, id 1680, seq 2, length 64
20:14:18.208010 IP (tos 0x0, ttl 64, id 3862, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.100 > 192.168.137.200: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 11771, offset 0, flags [none], proto ICMP (1), length 84)
    10.10.2.1 > 10.10.2.2: ICMP echo reply, id 1680, seq 2, length 64
20:14:19.209812 IP (tos 0x0, ttl 64, id 60184, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.200 > 192.168.137.100: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 28943, offset 0, flags [DF], proto ICMP (1), length 84)
    10.10.2.2 > 10.10.2.1: ICMP echo request, id 1680, seq 3, length 64
20:14:19.209953 IP (tos 0x0, ttl 64, id 4042, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.100 > 192.168.137.200: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 11890, offset 0, flags [none], proto ICMP (1), length 84)
    10.10.2.1 > 10.10.2.2: ICMP echo reply, id 1680, seq 3, length 64
20:14:20.211837 IP (tos 0x0, ttl 64, id 60377, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.200 > 192.168.137.100: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 29001, offset 0, flags [DF], proto ICMP (1), length 84)
    10.10.2.2 > 10.10.2.1: ICMP echo request, id 1680, seq 4, length 64
20:14:20.212008 IP (tos 0x0, ttl 64, id 4151, offset 0, flags [DF], proto GRE (47), length 108)
    192.168.137.100 > 192.168.137.200: GREv0, Flags [none], length 88
        IP (tos 0x0, ttl 64, id 12028, offset 0, flags [none], proto ICMP (1), length 84)
    10.10.2.1 > 10.10.2.2: ICMP echo reply, id 1680, seq 4, length 64
```

Commenter le résultat
La connectivité entre les deux interfaces du tunnel passe à travers le réseau réel (192.168.137.0/24)

e) Quels sont les inconvénients d'un tunnel GRE ? Dans quel cas ce type de tunnel peut être utile ?

Le tunnel GRE n'est pas sécurisé :

- GRE ne prévoit pas de chiffrement des données qui passent dans le tunnel;
- GRE ne prévoit pas l'authentification des extrémités du tunnel,

**Partie 2 : VPN site-à-site avec OpenVPN**

a) Supprimer le tunnel précédemment configuré sur la passerelle.

VPN_Server_1 et 2:

***sudo ip link set dev tun0 down***
***sudo ip tunnel del tun0***

```
user@ubuntu:~$ sudo ip link set dev tun0 down
user@ubuntu:~$ sudo ip tunnel del tun0
```

b) Créer une clé partagée de chiffrement avec OpenVPN sur une des passerelles, et copier cette clé sur l'autre passerelle (via la commande SSH : scp).
Valider le fonctionnement du tunnel à l'aide de commandes de diagnostique (affichage des adresses des interfaces, tables de routage, connexion client-à-client du tunnel).

VPN_Server_1 :

***openvpn –genkey –secret cle.key***

***scp cle.key user@192.168.137.200:/home/user***

```
user@ubuntu:~$ openvpn --genkey --secret cle.key
user@ubuntu:~$ scp cle.key user@192.168.137.200:/home/user
user@192.168.137.200's password:
cle.key                                       100%  636     0.6KB/s   00:00
```

VPN_Server_2: vérifier que la cle a été copiée

```
user@ubuntu:~$ ls
cle.key
```

c) Configurer un tunnel sécurisé entre les deux sites de l'entreprise à l'aide la clé partagée de chiffrement précédemment créée.

VPN_Server_1 :

***openvpn --remote 192.168.137.200 --dev tun0 --ifconfig 10.10.2.1 10.10.2.2 --secret cle.key***

```
user@ubuntu:~$ sudo openvpn --remote 192.168.137.200 --dev tun0 --ifconfig 10.10.2.1 10.10.2.2 --sec
ret  cle.key
```

VPN_Server_2

***openvpn --remote 192.168.137.100 --dev tun0 --ifconfig 10.10.2.2 10.10.2.1 --secret cle.key***

```
user@ubuntu:~$ sudo openvpn --remote 192.168.137.100 --dev tun0 --ifconfig 10.10.2.2 10.10.2.1 --sec
ret cle.key
```

d) Commenter la différence entre les deux méthodes.

Contrairement au protocole GRE, le protocole OPENVPN, utilise des algorithmes de chiffrement (AES) pour garantir la confidentialité et l'authentification entre les deux extrémités à travers une clé publique générée.