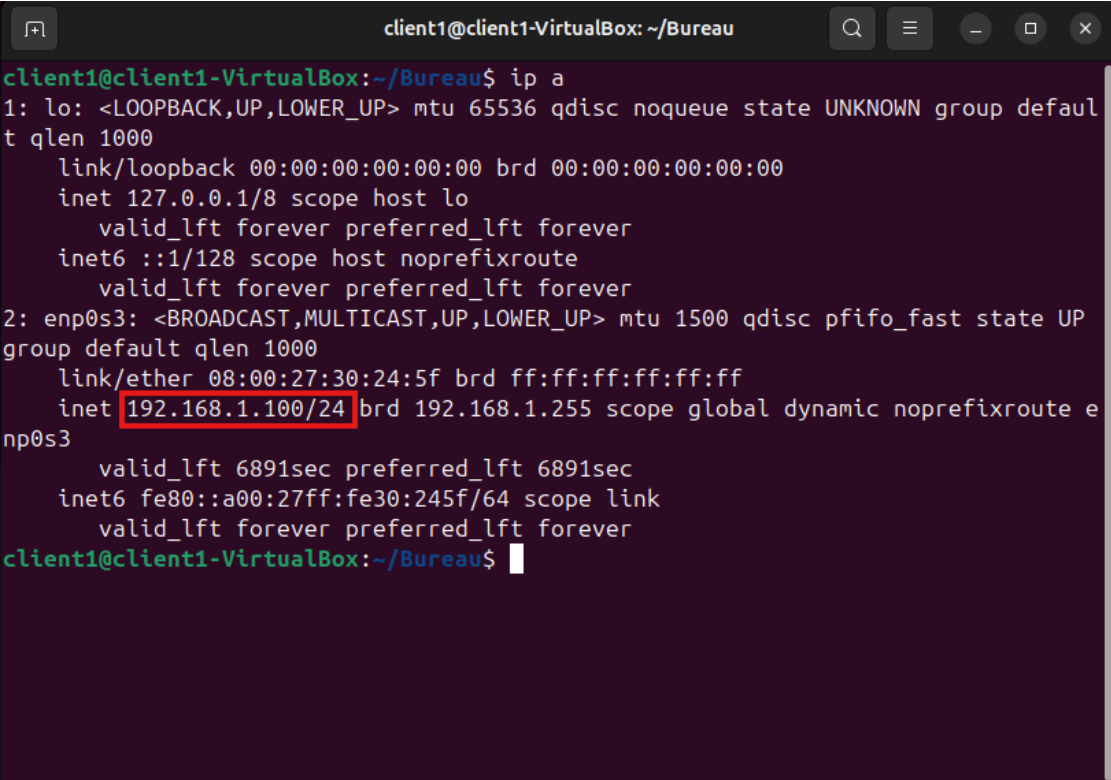


# Document d'exploitation

## I. Utilisation des services mis en place

Les services réseau ont été configurés pour fonctionner automatiquement une fois la machine cliente connectée à l'une des zones LAN. Chaque client reçoit automatiquement une adresse IP via DHCP et accéder aux services autorisés selon les règles du pare-feu. La configuration est conçue pour ne nécessiter aucune intervention manuelle côté utilisateur après la connexion.

### LAN1



```
client1@client1-VirtualBox: ~/Bureau
client1@client1-VirtualBox:~/Bureau$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:30:24:5f brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
        valid_lft 6891sec preferred_lft 6891sec
    inet6 fe80::a00:27ff:fe30:245f/64 scope link
        valid_lft forever preferred_lft forever
client1@client1-VirtualBox:~/Bureau$
```

## LAN2

```
client3@client3-VirtualBox: ~/Bureau
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

client3@client3-VirtualBox:~/Bureau$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:6c:4f:9e brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.101/24 brd 192.168.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 7125sec preferred_lft 7125sec
    inet6 fe80::a00:27ff:fe6c:4f9e/64 scope link
        valid_lft forever preferred_lft forever
client3@client3-VirtualBox:~/Bureau$
```

## Accès à internet:

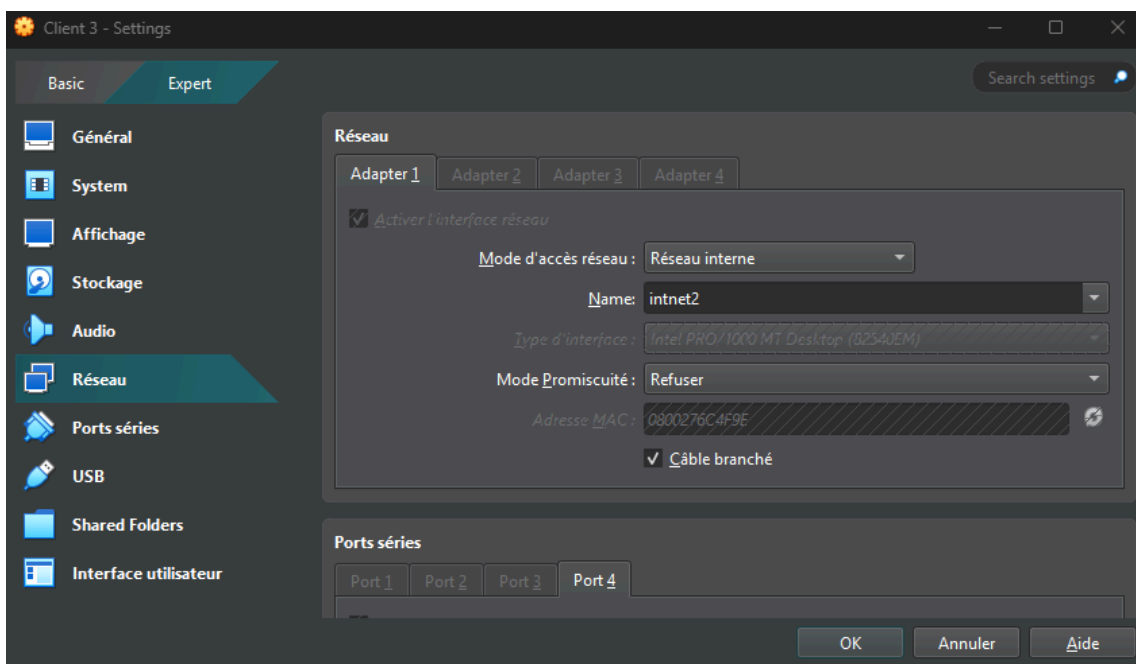
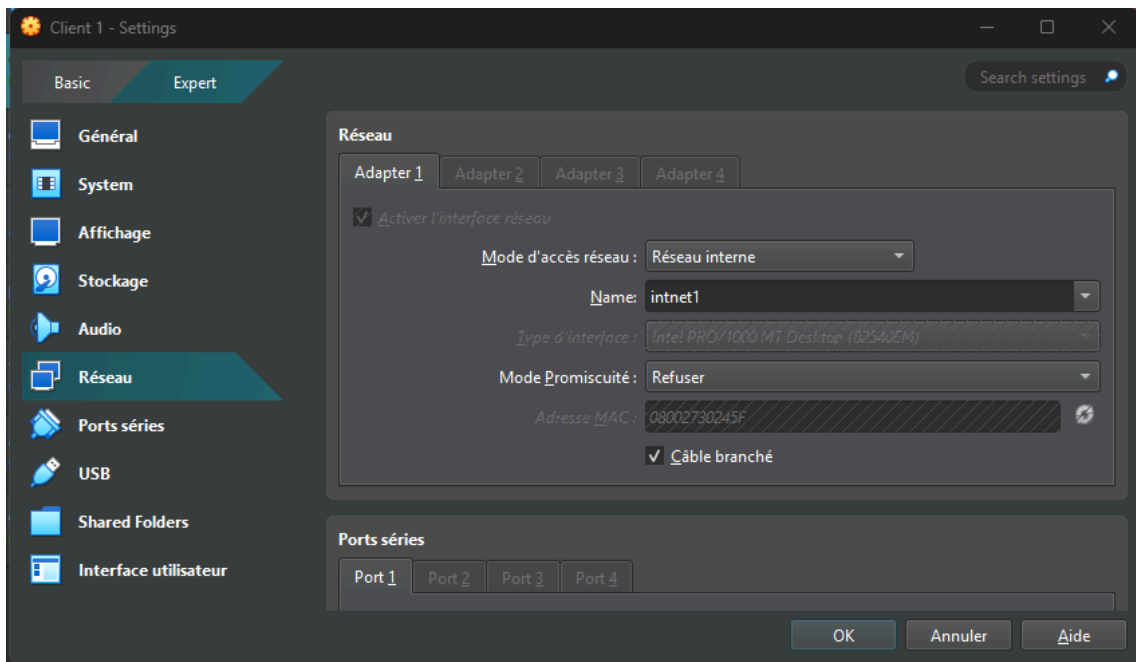
```
client1@client1-VirtualBox: ~/Bureau
client1@client1-VirtualBox:~/Bureau$ ping google.com
PING google.com (142.250.75.238) 56(84) bytes of data.
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp_seq=1 ttl=254 time=23.4 ms
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp_seq=2 ttl=254 time=30.4 ms
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp_seq=3 ttl=254 time=28.4 ms
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp_seq=4 ttl=254 time=29.7 ms
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp_seq=5 ttl=254 time=29.2 ms
64 bytes from par10s41-in-f14.1e100.net (142.250.75.238): icmp_seq=6 ttl=254 time=29.1 ms
^C
--- google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 9043ms
rtt min/avg/max/mdev = 23.445/28.371/30.435/2.289 ms
client1@client1-VirtualBox:~/Bureau$
```

## II. Intégrer LAN1 ou LAN2

Pour intégrer un poste client dans le LAN1 ou LAN2, il suffit d'assigner à la machine virtuelle le bon réseau interne dans VirtualBox :

- intnet1 pour LAN1
- intnet2 pour LAN2
- 

Une fois démarrée, la machine reçoit une adresse IP automatiquement via DHCP. Dans le cas de LAN1, le portail captif s'active pour forcer l'authentification avant tout accès.



### III. Communiquer

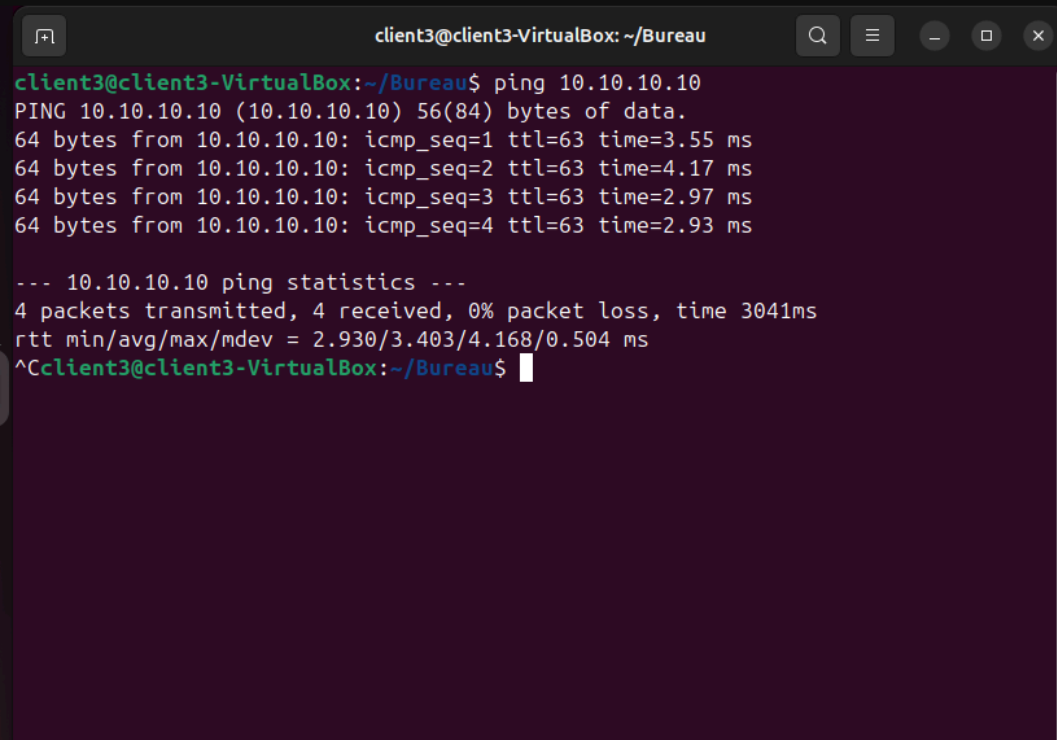
Les communications entre les machines suivent les règles définies dans pfSense :

- Les machines du LAN1 peuvent uniquement accéder à Internet après authentification.
- Les machines du LAN 2 peuvent accéder à Internet, à la DMZ, et pinguer certaines machines si autorisées.
- Le DMZ peut répondre aux requêtes mais ne peut pas initier de communication vers les LAN.

### IV. Accéder aux serveurs du DMZ

Depuis LAN2, il est possible d'accéder aux services hébergés dans la DMZ, comme un serveur web. L'accès se fait via l'adresse IP ou un nom interne configuré dans le DNS Resolver (ex : [web.local](#)). Cela permet de simuler un accès sécurisé à une zone exposée.

Échange à partir de LAN2 vers DMZ



```
client3@client3-VirtualBox: ~/Bureau
client3@client3-VirtualBox:~/Bureau$ ping 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=3.55 ms
64 bytes from 10.10.10.10: icmp_seq=2 ttl=63 time=4.17 ms
64 bytes from 10.10.10.10: icmp_seq=3 ttl=63 time=2.97 ms
64 bytes from 10.10.10.10: icmp_seq=4 ttl=63 time=2.93 ms

--- 10.10.10.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3041ms
rtt min/avg/max/mdev = 2.930/3.403/4.168/0.504 ms
^Cclient3@client3-VirtualBox:~/Bureau$
```

## Échange à partir de DMZ vers LAN2

```
dmz@dmz-VirtualBox: ~/Bureau
dmz@dmz-VirtualBox:~/Bureau$ ping 192.168.2.100
PING 192.168.2.100 (192.168.2.100) 56(84) bytes of data.
^C
--- 192.168.2.100 ping statistics ---
50 packets transmitted, 0 received, 100% packet loss, time 62802ms

dmz@dmz-VirtualBox:~/Bureau$
```

### V. Créer des utilisateurs dans le portail captif

L'interface de gestion du portail captif permet d'ajouter manuellement des utilisateurs depuis pfSense. Chaque compte dispose d'un identifiant et d'un mot de passe. Ces comptes permettent de contrôler qui peut accéder à Internet via le réseau LAN1. Une fois connectés, les utilisateurs sont redirigés automatiquement.

