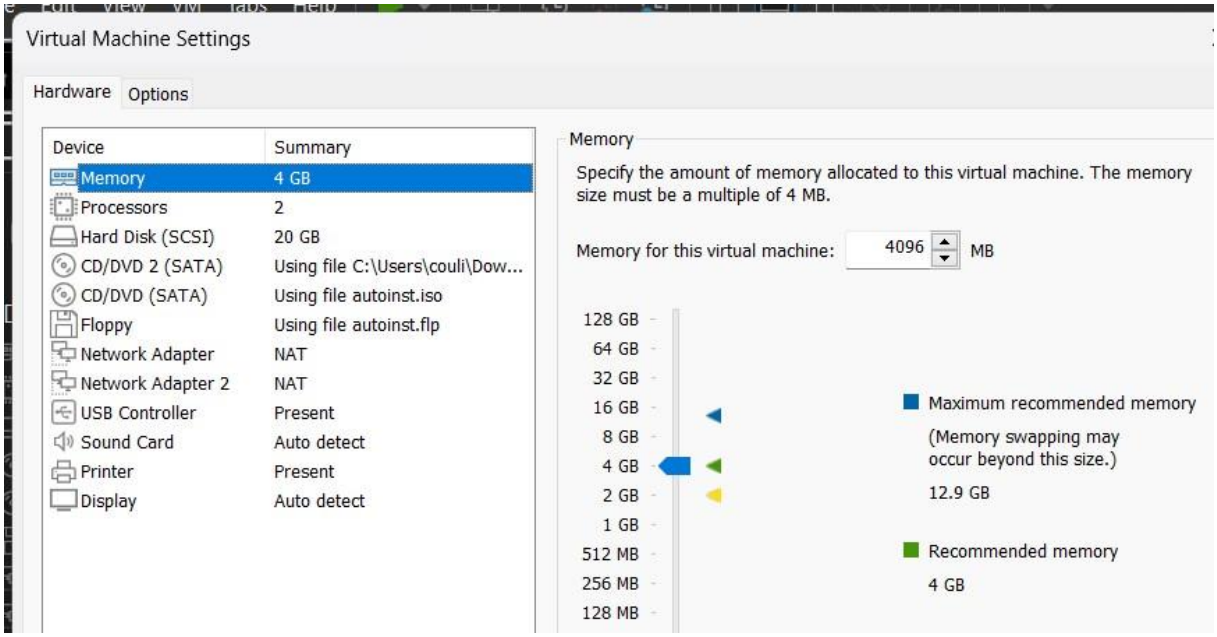
Rapport de TP - Sécurité des Réseaux

DEROULEMENT DU TP

Durant ce TP, nous avons travaillé avec des machines virtuelles Linux. Chaque groupe disposait de trois machines virtuelles, dont une agissant en tant que pare-feu. Voici le déroulement du TP :

I. Préparation des machines virtuelles :

- **Ajout d'une carte réseau à la machine Firewall :**
- 

Arrêt du système d'exploitation de la machine Firewall.

Sélection de la machine Firewall dans l'onglet "Inventory" de la VMware console.

Accès aux paramètres de la machine en cliquant droit sur "Firewall" et en sélectionnant "Setting" ou en passant par l'onglet "commands" puis "Edit virtual machine setting".

Ajout d'une carte réseau.

Redémarrage de la machine pour que l'utilitaire Kudzu détecte la nouvelle carte réseau.

- **Configuration des cartes réseau sous Linux :**

Utilisation de la commande ifconfig ou de l'interface graphique system-config-network pour vérifier et configurer l'adressage IP des machines.

```
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.10.1  netmask 255.255.255.0  broadcast 192.168.10.255
        inet6 fe80::2bf3:9ade:4621:fd6a  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3f:fa:7b  txqueuelen 1000  (Ethernet)
        RX packets 82873  bytes 120848564 (120.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24136  bytes 1517986 (1.5 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

ens37: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.21.0.1  netmask 255.255.255.0  broadcast 10.21.0.255
        inet6 fe80::cc51:1f52:953:4d80  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:3f:fa:85  txqueuelen 1000  (Ethernet)
        RX packets 3205  bytes 392548 (392.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1598  bytes 146589 (146.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 2098  bytes 183552 (183.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 2098  bytes 183552 (183.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

coulibably@coulibably-virtual-machine:~$
```

Test 1 :

Test de la commande ping entre chaque machine et le firewall, puis entre les deux machines.

Analyse des résultats et identification des raisons pour lesquelles le ping fonctionne dans certains cas et pas dans d'autres.

Ajout des configurations manquantes au niveau de chaque machine pour résoudre les problèmes de connectivité.

```
oulibably@coulibably-virtual-machine:~$ ping 192.168.232.130
ING 192.168.232.130 (192.168.232.130) 56(84) bytes of data.
4 bytes from 192.168.232.130: icmp_seq=1 ttl=64 time=1.75 ms
4 bytes from 192.168.232.130: icmp_seq=2 ttl=64 time=0.514 ms
4 bytes from 192.168.232.130: icmp_seq=3 ttl=64 time=0.509 ms
4 bytes from 192.168.232.130: icmp_seq=4 ttl=64 time=0.320 ms
4 bytes from 192.168.232.130: icmp_seq=5 ttl=64 time=0.583 ms
4 bytes from 192.168.232.130: icmp_seq=6 ttl=64 time=0.467 ms
4 bytes from 192.168.232.130: icmp_seq=7 ttl=64 time=0.362 ms
4 bytes from 192.168.232.130: icmp_seq=8 ttl=64 time=0.384 ms
4 bytes from 192.168.232.130: icmp_seq=9 ttl=64 time=0.468 ms
4 bytes from 192.168.232.130: icmp_seq=10 ttl=64 time=0.380 ms
4 bytes from 192.168.232.130: icmp_seq=11 ttl=64 time=0.459 ms
4 bytes from 192.168.232.130: icmp_seq=12 ttl=64 time=0.341 ms
4 bytes from 192.168.232.130: icmp_seq=13 ttl=64 time=0.435 ms
4 bytes from 192.168.232.130: icmp_seq=14 ttl=64 time=0.422 ms
4 bytes from 192.168.232.130: icmp_seq=15 ttl=64 time=0.387 ms
4 bytes from 192.168.232.130: icmp_seq=16 ttl=64 time=0.395 ms
C
-- 192.168.232.130 ping statistics ---
6 packets transmitted, 16 received, 0% packet loss, time 15318ms
tt min/avg/max/mdev = 0.320/0.510/1.746/0.325 ms
oulibably@coulibably-virtual-machine:~$ SSS
```

```
daouda@daouda-virtual-machine:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
^C
--- 192.168.10.1 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7145ms
```

```
daouda@daouda-virtual-machine:~$ ping 10.21.0.1
PING 10.21.0.1 (10.21.0.1) 56(84) bytes of data.
^C
--- 10.21.0.1 ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3070ms
```

```
coulibably@coulibably-virtual-machine:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
coulibably@coulibably-virtual-machine:~$
```

II. Configuration du Firewall :

- **Activation du routage :**

Modification du paramètre global de routage des paquets IP en écrivant la valeur 1 dans le fichier /proc/sys/net/ipv4/ip_forward.

```
coulibably@coulibably-virtual-machine:~$ cat /proc/sys/net/ipv4/ip_forward
0
```

```
coulibably@coulibably-virtual-machine:~$ echo "1" | sudo tee /proc/sys/net/ipv4/ip_forward
[sudo] password for coulibably:
1
```

Test de la connectivité après modification du paramètre.

- **Configuration du Firewall :**

Utilisation de la commande iptables pour lister la configuration actuelle du firewall.

Test 2 :

Analyse de la configuration par défaut du firewall.

Évaluation du rôle du firewall et de la sécurité des accès entre les deux réseaux.

```
coulibably@coulibably-virtual-machine:~$ sudo iptables -t filter -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request
ACCEPT     icmp --  anywhere             anywhere             icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
coulibably@coulibably-virtual-machine:~$
```

Test 3 :

Test du fonctionnement des protocoles HTTP, FTP et ICMP avec la configuration par défaut du Firewall.

Démarrage des services httpd et vsftpd sur la machine de destination.

```
coulibably@coulibably-virtual-machine:~$ service vsftpd start
coulibably@coulibably-virtual-machine:~$ ftp 192.168.232.130
ftp: Can't connect to `192.168.232.130:21': Connection refused
ftp: Can't connect to `192.168.232.130:ftp'
ftp>
```

```
coulibably@coulibably-virtual-machine:~$ ftp 192.168.232.130
Connected to 192.168.232.130.
220 (vsFTPd 3.0.5)
Name (192.168.232.130:coulibably):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> exit
221 Goodbye.
coulibably@coulibably-virtual-machine:~$ telnet 192.168.232.130 80
Trying 192.168.232.130...
telnet: Unable to connect to remote host: Connection refused
```

Utilisation des commandes ftp et telnet pour tester le fonctionnement des protocoles.

Conclusion :

Le TP a permis de comprendre les étapes de configuration d'un pare-feu sous Linux, ainsi que la gestion des règles de filtrage de paquets avec iptables. Nous avons également appris à tester la connectivité entre différentes machines et à évaluer la sécurité des accès à travers le pare-feu.