TP 6 – Routage & Firewall

I) Routage

1) Préliminaires

1)

```
kbalavoine@lespaul:~$ /sbin/route -n
Table de routage IP du noyau
Destination     Passerelle      Genmask         Indic Metric Ref    Use Iface
0.0.0.0         10.0.9.254      0.0.0.0         UG    0      0        0 eth0
10.0.9.0        0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

a)
Nous partageons effectivement le même réseau.

b)
l'ip de la route par défaut est 10.0.9.0

2)

```
kbalavoine@lespaul:~$ ip route ls
default via 10.0.9.254 dev eth0 onlink
10.0.9.0/24 dev eth0 proto kernel scope link src 10.0.9.18
```

/24 correspond au masque

3)

```
kbalavoine@lespaul:~$ ip -6 route ls
2001:660:6101:800:9::/80 dev eth0 proto kernel metric 256 pref medium
fe80::/64 dev eth0 proto kernel metric 256 pref medium
default via fe80::5a20:b1ff:feb1:2300 dev eth0 proto ra metric 1024 expires 8957sec hoplimit 25 pref medium
```

a)
la partie réseau correspond à ce qui tombe dans le /80, à savoir 2001:660:6101:800:9 et la partie machine correspond à ce qui vient après, ici 0 (donc pas affiché).

b)
On peut la voir sur la troisième ligne de la capture d'écran.

c)
On peut la voir sur la quatrième ligne de la capture d'écran.

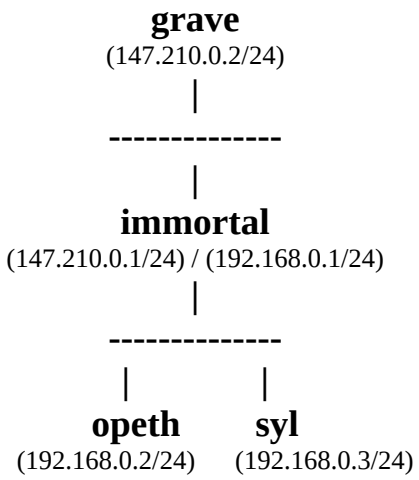
Memento Routage

En guise de documentation rapide, voici un résumé des commandes que l'on va utiliser dans les sections suivantes. Il n'y a donc pas d'action à faire dans cette section, c'est juste de la documentation. Il faut bien sûr remplacer `<@gateway>` par une adresse IP, etc.

- Activer le relai des paquets sur une machine (ip forward) :
  `echo 1 > /proc/sys/net/ipv4/ip_forward`
- Configurer de manière permanente le relai des paquets : voir le fichier `/etc/sysctl.conf`
- Afficher la table de routage : `route -n`
- Définir une route par défaut : `route add default gw <@gateway>`
- Ajouter une route vers un réseau spécifique :
  `route add -net <@network/bits> gw <@gateway>`
- Pour supprimer une règle, il faut taper la commande `route del <...>` avec exactement les mêmes arguments que pour la commande `add`.
- Vérifier la route envoyer un paquet à une adresse spécifique : `traceroute <@host>`
- On peut aussi utiliser la commande `ip` pour ajouter des route :
  `ip route add <@network/bits> via <@gateway>` (de même pour une seule adresse).

2) Routage Basique

1)



2)

les pings marchent

grave → immortal

```
root@grave:~# ping 147.210.0.1
PING 147.210.0.1 (147.210.0.1) 56(84) bytes of data.
64 bytes from 147.210.0.1: icmp_seq=1 ttl=64 time=0.540 ms
```

immortal → grave

```
root@immortal:~# ping 147.210.0.2
PING 147.210.0.2 (147.210.0.2) 56(84) bytes of data.
64 bytes from 147.210.0.2: icmp_seq=1 ttl=64 time=0.198 ms
```

immortal → opeth

```
root@immortal:~# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=0.203 ms
```

opeth → immortal

```
root@opeth:~# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=0.347 ms
```

opeth → syl

```
root@opeth:~# ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
64 bytes from 192.168.0.3: icmp_seq=1 ttl=64 time=0.230 ms
```

3)

grave :

```
root@grave:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

immortal :

```
root@immortal:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

opeth :

```
root@opeth:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

syl :

```
root@syl:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

4)

grave :

```
root@grave:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.0.1     0.0.0.0         UG    0      0        0 eth0
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

immortal :

```
root@immortal:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
147.210.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

opeth :

```
root@opeth:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

syl :

```
root@syl:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.0.1     0.0.0.0         UG    0      0        0 eth0
192.168.0.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

5)
opeth → grave (vue depuis immortal)

```
root@immortal:~# tcpdump -n -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bys
15:37:09.951654 ARP, Request who-has 192.168.0.1 tell 192.168.0.2, length 46
15:37:09.951673 ARP, Reply 192.168.0.1 is-at aa:aa:aa:aa:00:01, length 28
^C
2 packets captured
2 packets received by filter
0 packets dropped by kernel
root@immortal:~# tcpdump -n -i any
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on any, link-type LINUX_SLL (Linux cooked v1), capture size 262144 bys
15:37:21.818284 IP 192.168.0.2 > 147.210.0.2: ICMP echo request, id 582, seq 1,4
15:37:21.818295 IP 192.168.0.2 > 147.210.0.2: ICMP echo request, id 582, seq 1,4
15:37:21.819469 IP 147.210.0.2 > 192.168.0.2: ICMP echo reply, id 582, seq 1, l4
15:37:21.819472 IP 147.210.0.2 > 192.168.0.2: ICMP echo reply, id 582, seq 1, l4
15:37:26.830691 ARP, Request who-has 147.210.0.1 tell 147.210.0.2, length 46
15:37:26.830708 ARP, Reply 147.210.0.1 is-at aa:aa:aa:aa:00:00, length 28
```

3) Routage Avancée

opeth :

```
root@opeth:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.12.2    0.0.0.0         UG    0      0        0 eth0
147.210.12.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

immortal :

```
root@immortal:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.13.2    0.0.0.0         UG    0      0        0 eth1
147.210.12.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
147.210.13.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

grave :

```
root@grave:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
147.210.12.0    147.210.13.1    255.255.255.0   UG    0      0        0 eth0
147.210.13.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
147.210.14.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
147.210.15.0    147.210.14.2    255.255.255.0   UG    0      0        0 eth1
```

syl :

```
root@syl:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.14.1    0.0.0.0         UG    0      0        0 eth0
147.210.14.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
147.210.15.0    0.0.0.0         255.255.255.0   U     0      0        0 eth1
```

nile :

```
root@nile:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         147.210.15.1    0.0.0.0         UG    0      0        0 eth0
147.210.15.0    0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

opeth → nile

```
root@opeth:~# ping 147.210.15.2
PING 147.210.15.2 (147.210.15.2) 56(84) bytes of data.
64 bytes from 147.210.15.2: icmp_seq=1 ttl=61 time=2.54 ms
```

II) Firewall

La DMZ est une zone tampon entre internet et le réseau d'entreprise. Cela veut dire qu'elle est un par-feu pour le réseau interne, limitant ainsi les risques.
Le réseau d'entreprise lui contient tous les fichiers internes à l'entreprise, et où tout opération intérieur est mené.

1)
passerelle immortal (test avec deux versions) :

```
root@immortal:~# iptables -A FORWARD -s 192.168.1.0/24 -p icmp -j ACCEPT
root@immortal:~# iptables -D FORWARD -s 192.168.1.0/24 -p icmp -j ACCEPT
root@immortal:~# iptables -A FORWARD -i eth2 -p icmp -j ACCEPT
```

2)
nile → grave :

```
root@nile:~# ping 172.16.0.2
PING 172.16.0.2 (172.16.0.2) 56(84) bytes of data.
64 bytes from 172.16.0.2: icmp_seq=1 ttl=63 time=0.525 ms
64 bytes from 172.16.0.2: icmp_seq=2 ttl=63 time=1.59 ms
64 bytes from 172.16.0.2: icmp_seq=3 ttl=63 time=1.62 ms
^C
--- 172.16.0.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
```

grave → nile :

```
root@grave:~# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
^C
--- 192.168.1.2 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2000ms
```

3)

```
root@immortal:~# iptables -A FORWARD -i eth2 -p tcp --dport 80 -j ACCEPT
```

nile → grave :

```
root@nile:~# wget 172.16.0.2
--2023-11-23 16:28:27--  http://172.16.0.2/
Connecting to 172.16.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10701 (10K) [text/html]
Saving to: 'index.html'

index.html          100%[===================>]  10.45K  --.-KB/s    in 0s

2023-11-23 16:28:27 (218 MB/s) - 'index.html' saved [10701/10701]
```

nile → opeth :

```
root@nile:~# wget 147.210.0.2
--2023-11-23 16:32:04--  http://147.210.0.2/
Connecting to 147.210.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10701 (10K) [text/html]
Saving to: 'index.html.2'

index.html.2        100%[===================>]  10.45K  --.-KB/s    in 0s

2023-11-23 16:32:04 (260 MB/s) - 'index.html.2' saved [10701/10701]
```

4)

```
root@immortal:~# iptables -A FORWARD -i 172.16.0.2 -d 192.168.0.3 -p tcp --dport 22 -j ACCEPT
toto@grave:~$ ssh 192.168.0.3
The authenticity of host '192.168.0.3 (192.168.0.3)' can't be established.
ECDSA key fingerprint is SHA256:b2tuLYwJkZtgLmH5GkvZyi2JWc/v8plfeyPmuz9cxmU.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.3' (ECDSA) to the list of known hosts.
toto@192.168.0.3's password:
Linux dt 4.7.0-1-amd64 #1 SMP Debian 4.7.2-1 (2016-08-28) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
toto@dt:~$
```

Je suis bien connecté à dt depuis grave

5)

```
root@immortal:~# iptables -A FORWARD -d 192.168.0.2 -p tcp --dport 80 -j ACCEPT
root@grave:~# wget 192.168.0.2
--2023-11-23 16:54:04--  http://192.168.0.2/
Connecting to 192.168.0.2:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10701 (10K) [text/html]
Saving to: 'index.html'

index.html          100%[===================>]  10.45K  --.-KB/s    in 0s

2023-11-23 16:54:04 (223 MB/s) - 'index.html' saved [10701/10701]
```

6)

Premier test (opeth → eth1) :

```
root@opeth:~# nmap 192.168.0.0/24 -PN

Starting Nmap 7.12 ( https://nmap.org ) at 2023-11-23 16:58 UTC
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Stats: 0:01:08 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.53% done
Stats: 0:01:12 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.56% done
Stats: 0:01:16 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.59% done
Stats: 0:01:18 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.61% done
Stats: 0:01:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.70% done
Stats: 0:02:18 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.08% done; ETC: 20:31 (3:31:02 remaining)
Stats: 0:02:51 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 1.34% done; ETC: 20:31 (3:30:29 remaining)
```

j'ai arrêté après 3 minutes.

opeth → syl :

```
root@opeth:~# nmap -PN 192.168.0.2

Starting Nmap 7.12 ( https://nmap.org ) at 2023-11-24 15:29 UTC
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.2
Host is up (0.00065s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 8.86 seconds
```

opeth → dt :

```
root@opeth:~# nmap -PN 192.168.0.3

Starting Nmap 7.12 ( https://nmap.org ) at 2023-11-24 15:36 UTC
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.3
Host is up.
All 1000 scanned ports on 192.168.0.3 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.27 seconds
```

grave → syl :

```
root@grave:~# nmap -PN 192.138.0.2

Starting Nmap 7.12 ( https://nmap.org ) at 2023-11-24 15:36 UTC
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.138.0.2
Host is up.
All 1000 scanned ports on 192.138.0.2 are filtered

Nmap done: 1 IP address (1 host up) scanned in 201.30 seconds
```

grave → dt :

```
root@grave:~# nmap -PN 192.168.0.3

Starting Nmap 7.12 ( https://nmap.org ) at 2023-11-24 15:29 UTC
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.3
Host is up (0.0015s latency).
Not shown: 999 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 8.32 seconds
```

On peut ici voir plusieurs choses :

- opeth/syl n’ouvre que http
- grave/dt n’ouvre que ssh
- opeth/dt et grave/syl sont bloqués, ils n’ouvrent rien.