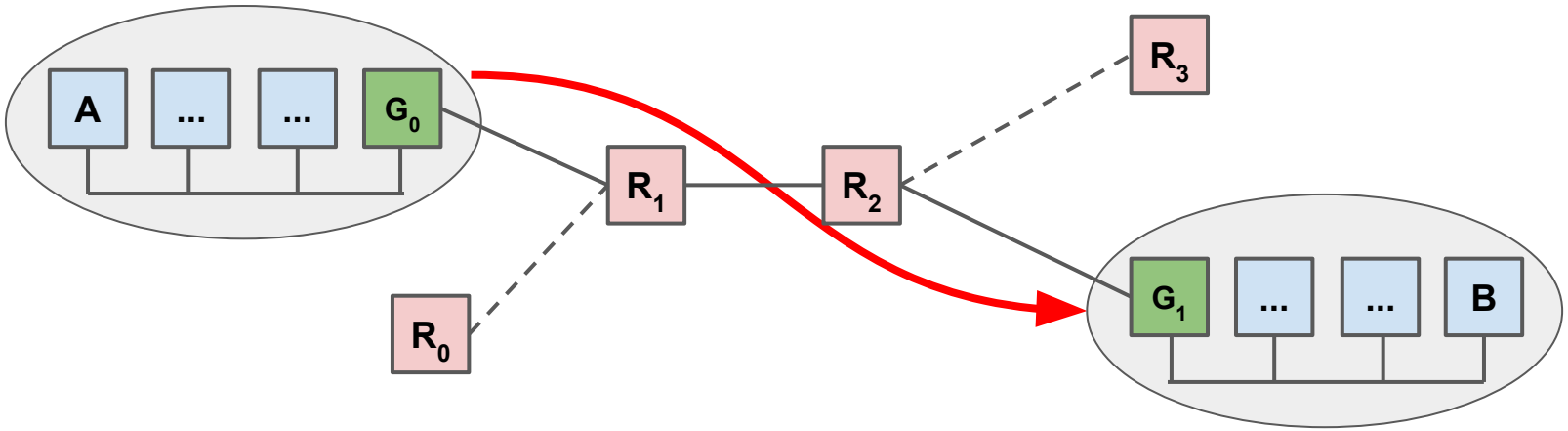
Cours 6.A

Routage

Rappel sur le Routage IP

Principe : Mécanisme par lequel un paquet IP est acheminé d'un expéditeur (A) jusqu'à son destinataire (B), en s'appuyant sur les noeuds intermédiaires (Gi, Ri) du réseau Internet.

Les différents noeuds du réseau : les hôtes (A,B), les passerelles ou *gateway* (G_i) et les routeurs (R_i)



Routage statique & dynamique : manuel, DHCP, OSPF, BGP, ...

Routage Statique Simple

Configuration dans le réseau 192.168.10.0/24 de la machine D comme passerelle vers Internet...

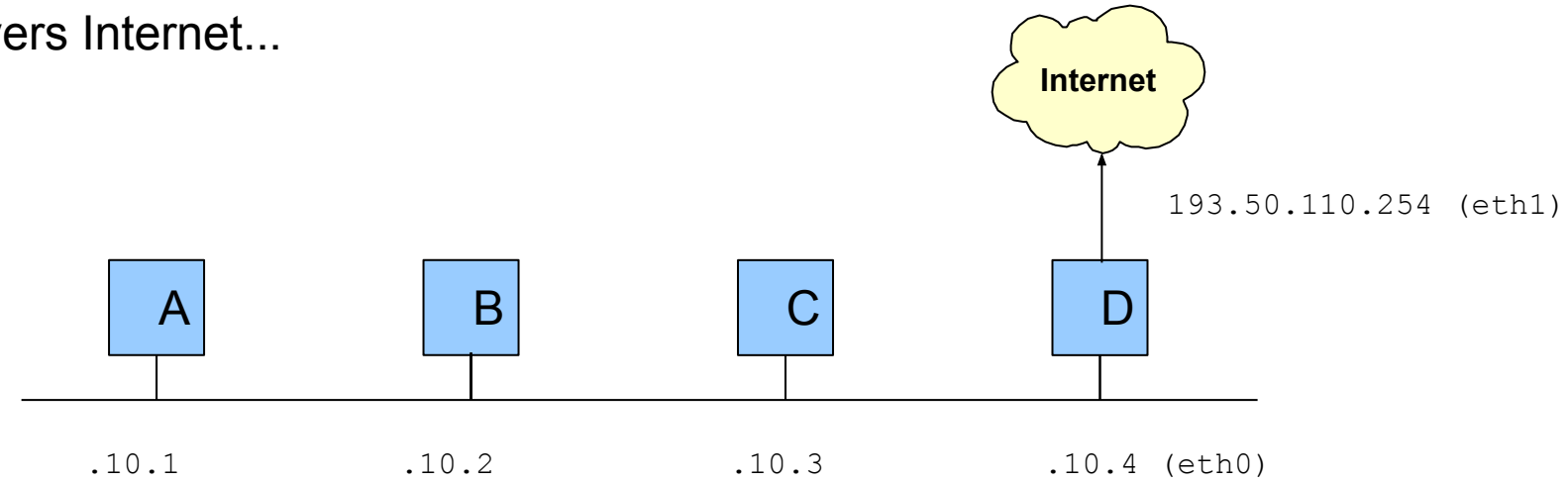


Table de routage attendue pour les machines hôtes (A, B, C) du LAN :

```
$ route -n
DestAddr        Gateway         GenMask         Flags   Interface
192.168.10.0    *               255.255.255.0   U       eth0
default         192.168.10.4    0.0.0.0         UG      eth0
```

- En bleu, route directe configurée implicitement par *ifconfig eth0…*
- En rouge, la route par défaut qu'il faut ajouter explicitement en indiquant l'adresse de la passerelle

Routage Statique Simple : Configuration

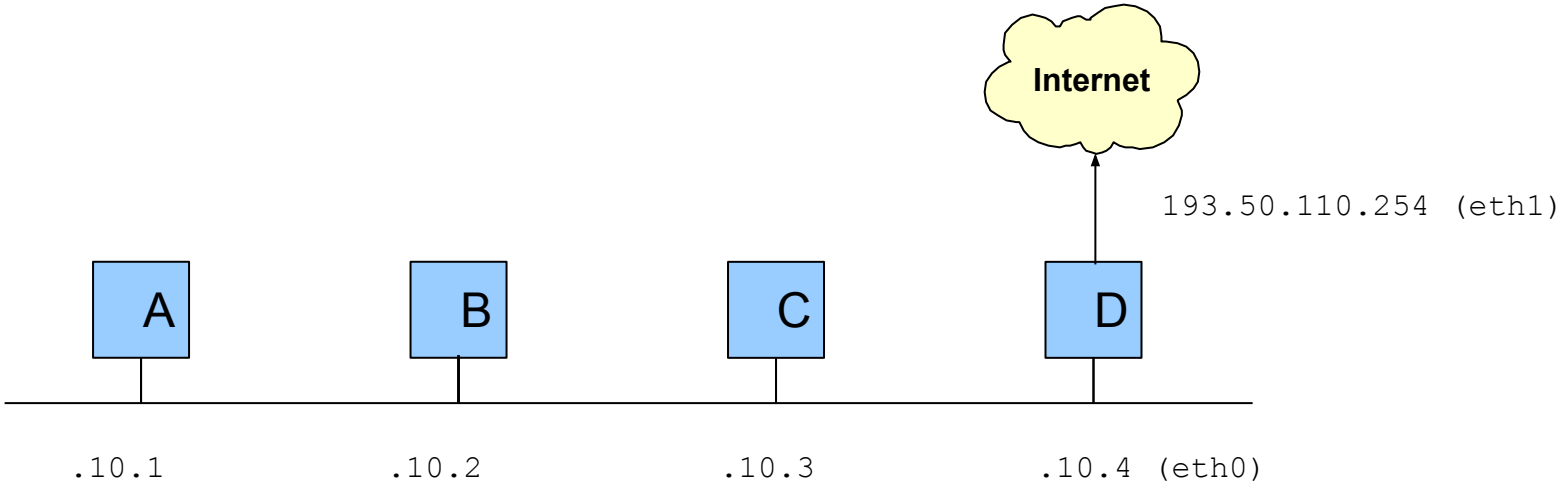
Configuration d'une passerelle D pour le réseau 192.168.10.0/24 permettant d'accéder à Internet

Activer la machine D comme passerelle (IP Forward)

```
$ echo 1 >  /proc/sys/net/ipv4/ip_forward
```

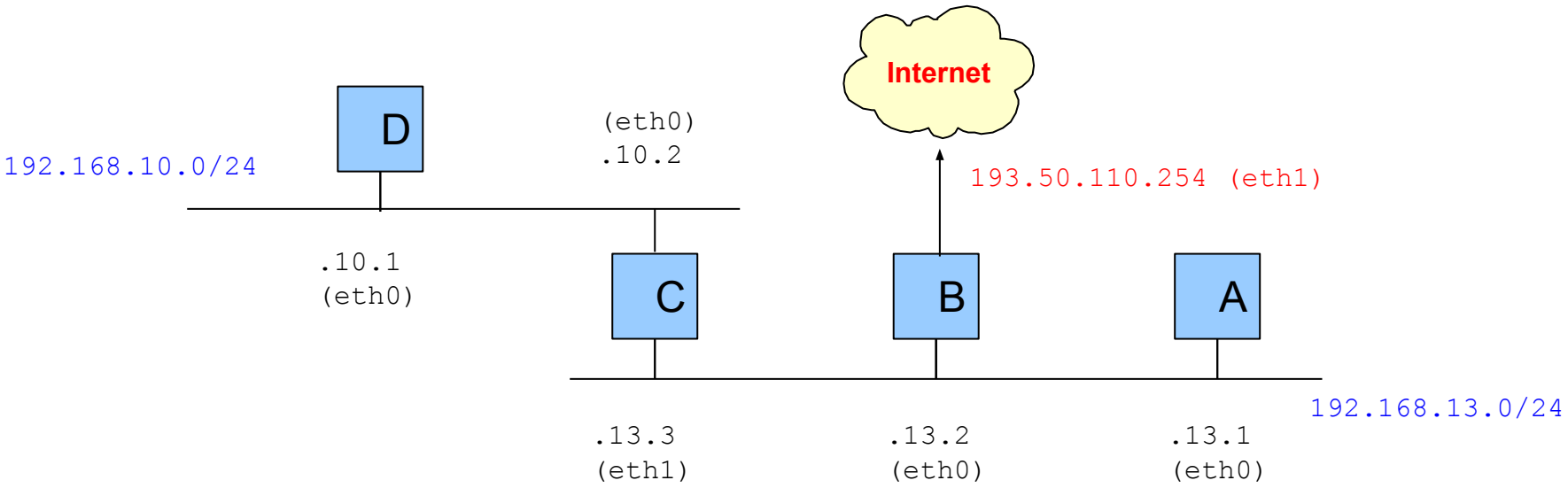
Configuration d'une route par défaut vers l'extérieur pour A, B, C, ...

```
$ route add default gw 192.168.10.4
```



Routage Statique

Considérons le réseau suivant.



Exercice.

- Lister les machines dans chaque réseau local.
- Pour chaque réseau/machine, indiquez les différentes passerelles.
- Ecrire la table de routage des machines A et D au format suivant :

  DestAddr, Gateway, GenMask, Flags, Interface

Routage Statique

Correction.

- Dans le réseau local 192.168.10.0/24, on trouve les machines D et C. La machine C est la paserelle vers l'autre LAN et Internet.
  - Ajout d'une route par défaut
- Dans le réseau local 192.168.13.0/24, on trouve les machines A, B, C. La machine B est la passerelle vers Internet, et la machine C est la passerelle vers l'autre LAN.
  - Ajout d'une route par défaut vers Internet et d'un route spécifique vers l'autre LAN
- Tables de routage des machines A et D

A$ route -n

DestAddr	*Gateway*	*GenMask*	*Flags*	*Interface*
192.168.13.0	*	255.255.255.0	U	eth0
192.168.10.0	192.168.13.3	255.255.255.0	U	eth0
default	192.168.13.2	0.0.0.0	UG	eth0

D$ route -n

DestAddr	*Gateway*	*GenMask*	*Flags*	*Interface*
192.168.10.0	*	255.255.255.0	U	eth0
default	192.168.10.2	0.0.0.0	UG	eth0

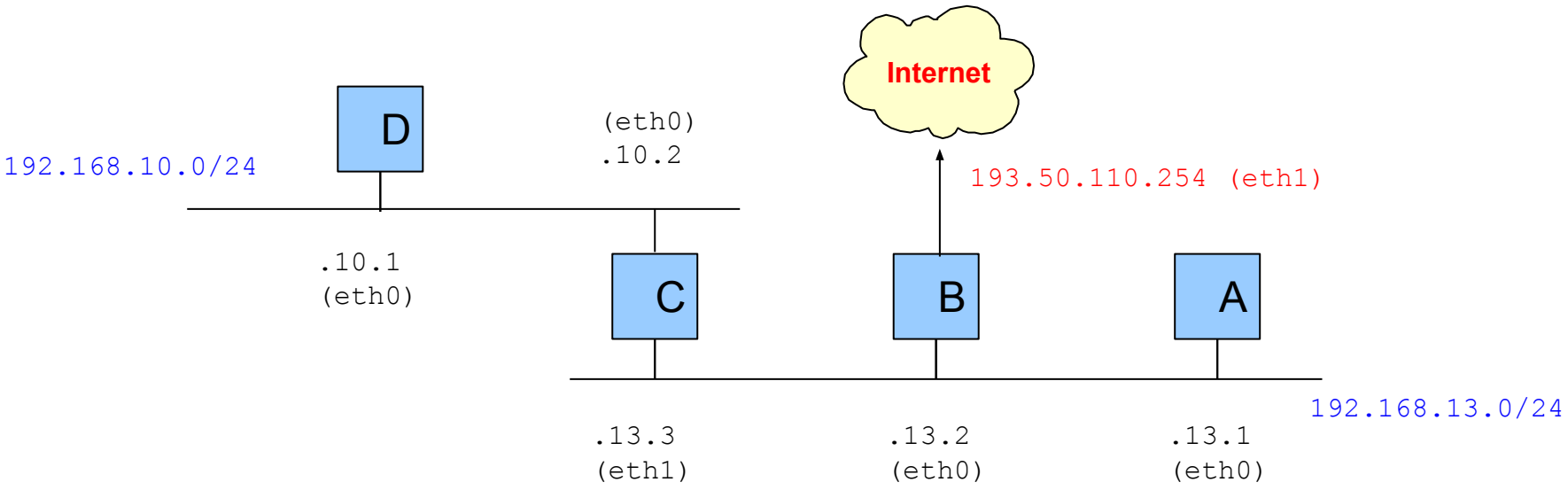
Routage Statique : Configuration

Pour les machines de 192.168.10.0/24, C joue le rôle de passerelle par défaut

```
D$ route add default gw 192.168.10.2
```

Pour 192.168.13.0/24, C joue le rôle de passerelle vers 192.168.10.0/24 et B joue le rôle de passerelle par défaut

```
A$ route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.13.3
A$ route add default gw 192.168.13.2
...
```



Routage : Memento

Activer le routage sur une machine (ip forward)

```
$ echo 1 > /proc/sys/net/ipv4/ip_forward
$ sysctl -w net.ipv4.ip_forward=1            # /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 ou une machine particulière

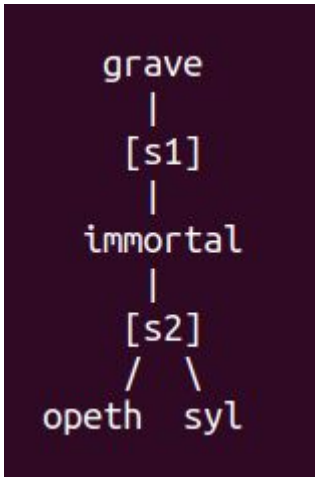
```
$ route add -net <@network> netmask <mask> gw <@gateway>
$ route add -host <@host> gw <@gateway>
```

Pour supprimer une règle, il faut taper la commande *route del* avec exactement les mêmes arguments que pour la commande *route add*.

Routage : Démo

Configurez les IP du réseau suivant.

```
opeth$ ifconfig eth0 192.168.0.2/24
syl$ ifconfig eth0 192.168.0.3/24
immortal$ ifconfig eth1 192.168.0.1/24
immortal$ ifconfig eth0 147.210.0.1/24
grave$ ifconfig eth0 147.210.0.2/24
```



qemunet/demo/gw.topo

Configurez le routage

```
opeth$ route add default gw 192.168.0.1
syl$ route add default gw 192.168.0.1
grave$ route add default gw 147.210.0.1
immortal$ echo 1 > /proc/sys/net/ipv4/ip_forward
```

Test de ping entre *opeth* et *grave*

```
opeth$ ping 147.210.0.2
64 bytes from 147.210.0.2: icmp_seq=1 ttl=63 time=0.413 ms
```

```
immortal$ tcpdump -i any
12:06:10.856698 IP 192.168.0.2 > 147.210.0.2: ICMP echo request, id 515, seq 480, length 64
12:06:10.856723 IP 192.168.0.2 > 147.210.0.2: ICMP echo request, id 515, seq 480, length 64
12:06:10.857277 IP 147.210.0.2 > 192.168.0.2: ICMP echo reply, id 515, seq 480, length 64
12:06:10.857285 IP 147.210.0.2 > 192.168.0.2: ICMP echo reply, id 515, seq 480, length 64
```

Routage : Exercice en TP

Exercice. Considérons le réseau 147.210.0.0/16 avec la configuration suivante. On distingue 4 sous-réseaux interconnectés par les switchs *s1, s2, s3* et *s4*.

```
opeth - [s1] - immortal - [s2] - grave - [s3] -  syl -  [s4] - nile
```

- Sur quelle machine faut-il activer le *forward* de paquet IP ?

  Sur *immortal, grave,* et *syl* qui servent de passerelles entre deux sous-réseaux. Ce n'est pas le cas pour *opeth* et *nile* qui n'appartiennent que à un seul sous-réseau.

- Quelle est la route par défaut pour *opeth* ?

  C'est @*immortal* dans le réseau local d'*opeth*. De même pour *nile* avec *syl* comme passerelle.

- Est-ce qu'une route par défaut est suffisante pour *immortal* ? Même question pour *grave*.

  Oui pour *immortal*. En effet, *immortal* peut parler directement à *opeth* et *grave*, mais nécessite d'utiliser *grave* comme passerelle pour parler aux réseaux *s3* et *s4*.

  Non pour *grave*. Dans ce cas précis, il faut ajouter deux routes spécifiques vers les réseaux *s1* et *s4* avec *route add -net* …

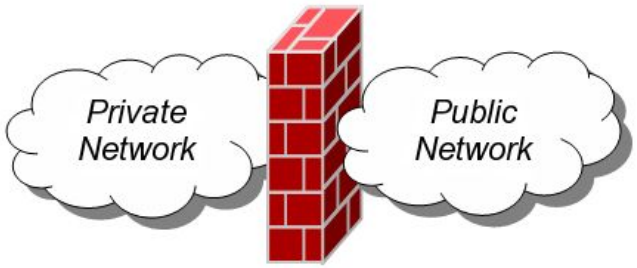
Cours 6.B

Firewall

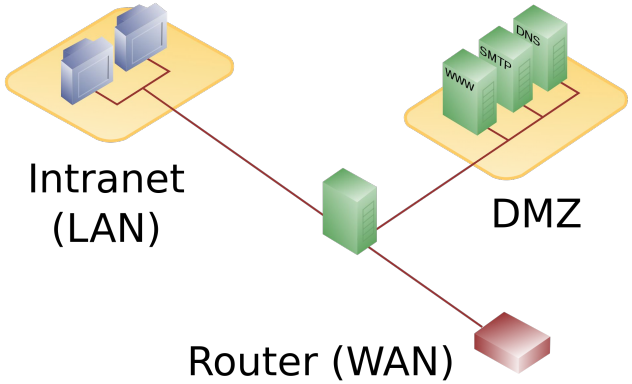
Firewall

Firewall (ou pare-feu) : logiciel contrôlant le traffic réseau en filtrant les paquets entrant & sortant selon une politique de sécurité (ex. iptables)

- **Politique de sécurité** : ensemble de règles détaillant les communications autorisées.
- **Politique par défaut** : toute communication non autorisée explicitement est rejetée !
- Protéger l'accès au réseau privé et sensible de l'entreprise (**Intranet**)
- Les services publics "à risques" (ouverts vers l'extérieur) sont isolés dans le réseau **DMZ** (ou zone démilitarisée) : serveurs web, mail, …



Source : wikipedia.



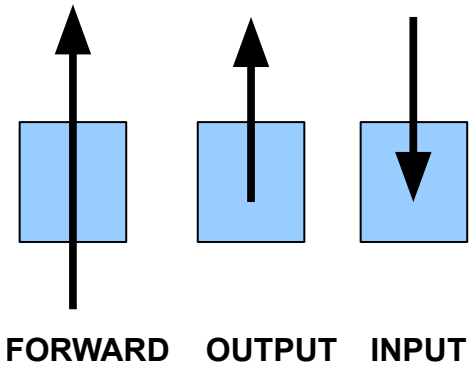
Configuration du Firewall avec iptables

Lister les règles

```
$ iptables -L -v
```

Remise à zéro (*flush*)

```
$ iptables -F
```



Ajouter une nouvelle règle avec -A (supprimer avec -D)

```
$ iptables -A <CHAIN> <SRC> <DST> <...> -j <ACTION>
```

Politique par défaut (si aucune règle ne s'applique avant)

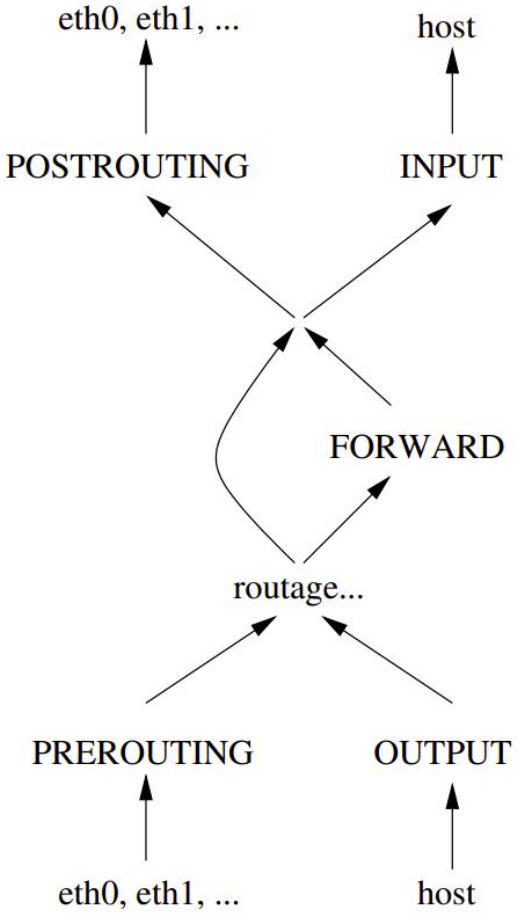
```
$ iptables -P <CHAIN> <ACTION>   # <ACTION> = ACCEPT | DROP
```

Memento

```
<CHAIN> = FORWARD | INPUT | OUTPUT
<ACTION> = ACCEPT | REJECT | DROP
<SRC> = -i eth0 | -s 192.168.0.1 | -s 192.168.0.0/24
<DST> = -o eth0 | -d 192.168.0.1 | -d 192.168.0.0/24
<...> = -p icmp | -p tcp --dport 80 | -m state --state <STATE>
<STATE> = NEW | ESTABLISHED | RELATED | INVALID
* NEW : établissement d'une nouvelle connexion
* ESTABLISHED : une connexion déjà établie
```

Configuration du Firewall avec iptables

Principe général



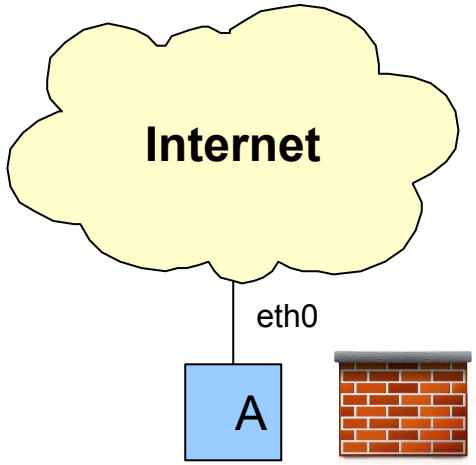
Firewall : protéger une machine

Comment protéger une machine directement reliée à Internet ?

On configure le firewall de A pour les *chains* INPUT & OUPUT.

On interdit tout par défaut...

```
$ iptables -P INPUT DROP
$ iptables -P OUTPUT DROP
```



On autorise le ping !

```
$ iptables -A INPUT -p icmp -j ACCEPT
$ iptables -A OUTPUT -p icmp -j ACCEPT
```

On autorise uniquement l'accès de A au web...

```
$ iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
⇒ NEW + ESTABLISED autorisés...
```

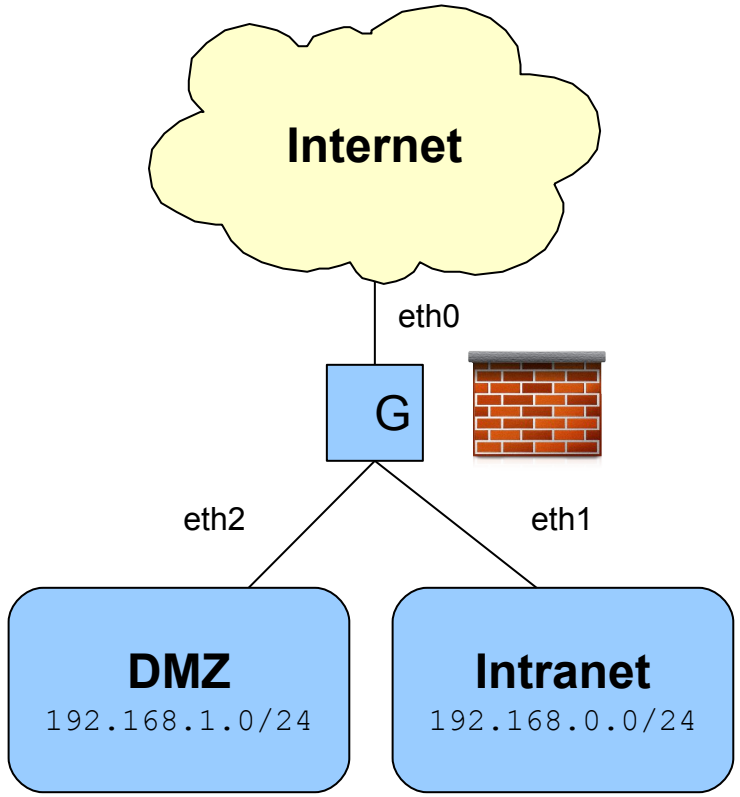
Et le traffic retour :

```
$ iptables -A INPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
⇒ NEW est donc interdit !!!
```

Firewall : protéger un réseau privé

Comment protéger un réseau privé relié à Internet via une passerelle ?

- On configure le firewall sur la passerelle G pour la *chain* FORWARD.
- Les services “à risques” sont mis dans le sous-réseau DMZ, séparé physiquement de l’Intranet.



Firewall : protéger un réseau privé

On interdit tout par défaut…

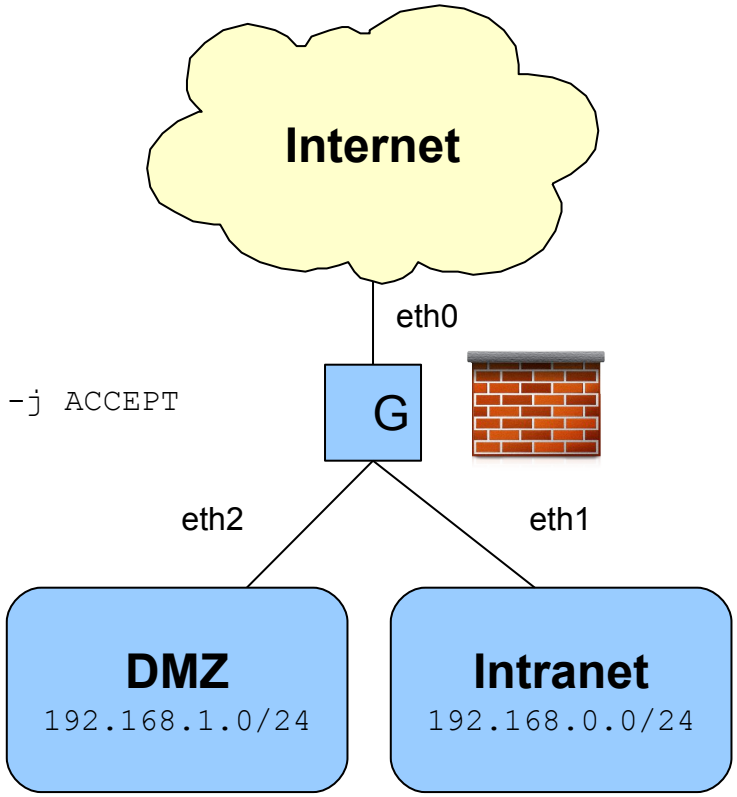
```
$ iptables -P FORWARD DROP
```

On autorise l'accès au serveur web 192.168.1.100 dans la DMZ

```
$ iptables -A FORWARD -d 192.168.1.100 -p tcp --dport 80 -j ACCEPT
$ iptables -A FORWARD -s 192.168.1.100 -p tcp --sport 80
           -m state --state ESTABLISHED -j ACCEPT
```

On autorise tout le traffic sortant de l'Intranet…

```
$ iptables -A FORWARD -s 192.168.0.0/24 -j ACCEPT
$ iptables -A FORWARD -d 192.168.0.0/24
           -m state --state ESTABLISHED -j ACCEPT
```

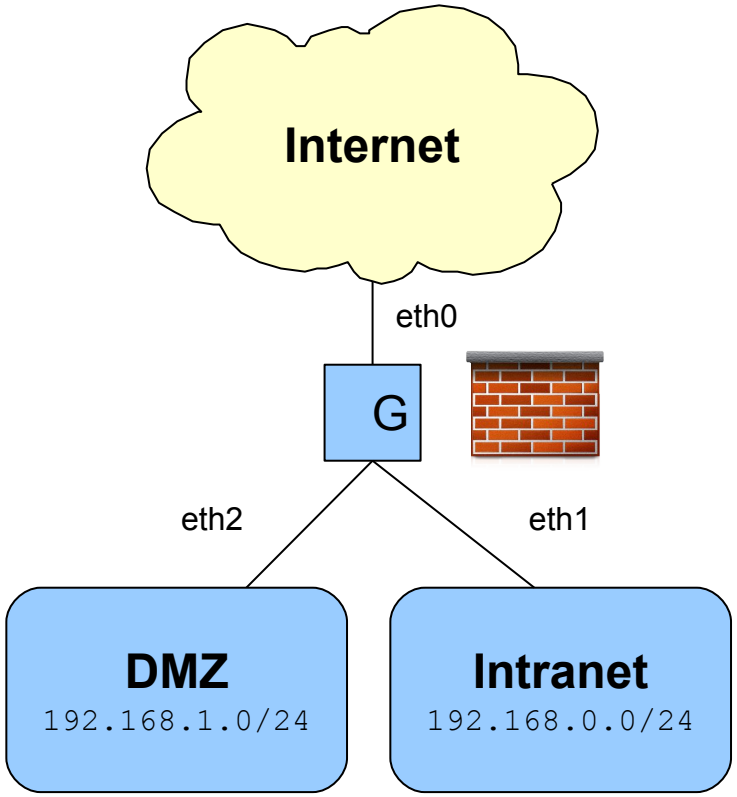


Mais on interdit tout accès entrant à l'Intranet, sauf SSH.

```
$ iptables -A FORWARD -d 192.168.0.0/24 -p tcp --dport 22 -j ACCEPT
$ iptables -A FORWARD -S 192.168.0.0/24 -p tcp --sport 22
           -m state --state ESTABLISHED -j ACCEPT
```

Firewall : protéger un réseau privé

Exercice : Ajoutez une régle pour permettre aux utilisateurs de l'Intranet de se connecter dans la DMZ par SSH.



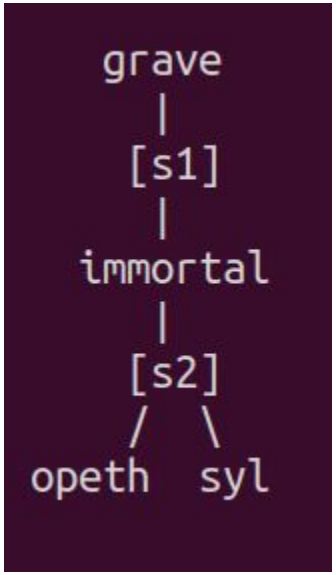
Firewall : protéger un réseau privé

Correction

```
$ iptables -A FORWARD -s 192.168.0.0/24 -d 192.168.1.0/24 -p tcp --dport 22 -j ACCEPT
$ iptables -A FORWARD -d 192.168.0.0/24 -s 192.168.1.0/24 -p tcp --sport 22
           -m state --state ESTABLISHED -j ACCEPT
```

Démo

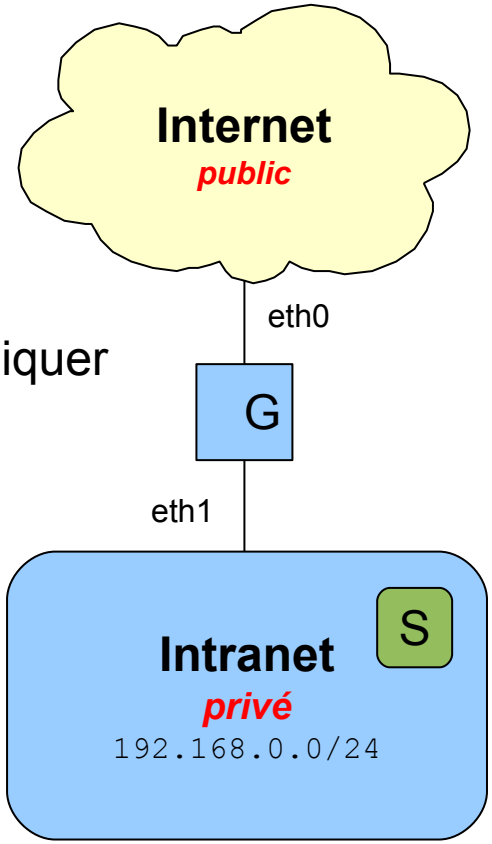
- Tester le ping entre *opeth* et *grave*
- Mettre en place un firewall sur *immortal* avec un politique par défaut à DROP
- Vérifer que le ping ne marche plus…
- Modifier le firewall pour autoriser ICMP dans les deux sens
- Modifier le firewall pour autoriser *opeth* à se connecter à *grave* en SSH (TCP/22) avec le compte utilisateur *toto*



NAT

NAT (Network Address Translation)

- Un réseau privé ne peut pas accéder et n'est pas accessible depuis Internet (adresses IP non routables)
- Mais possibilité d'utiliser une passerelle NAT !



NAT dynamique : les machines de l'Intranet peuvent communiquer sur Internet en empruntant l'adresse publique de G

```
G$ iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Port-Forwarding : on souhaite rendre accessible sur Internet le serveur web S (192.168.0.100, port 8080) en utilisant un transfert de port de G:80 vers S:8080

```
G$ iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80
            -j DNAT --to 192.168.0.100:8080
```

Redirect

TODO