

# Les pare-feux

- ★ Définition
- ★ Principes de fonctionnement
- ★ Application à iptables

# Définition

- ★ Un pare-feu est un logiciel qui :
  - Analyse les trames qu'il reçoit et prend une décision en fonction des adresses de couche 2, 3 et 4 => filtrage sans état
  - La décision peut être prise en fonction de l'état d'une connexion et/ou des drapeaux TCP => filtrage dynamique
  - La décision peut être prise en fonction du contenu de couche 7 => filtrage applicatif

# Logiciels libres

- **Linux Netfilter/Iptables**, pare-feu libre des noyaux Linux 2.4 et 2.6.
- **Linux Ipchains**, pare-feu libre du noyau Linux 2.2.
- **Packet Filter** ou PF, pare-feu libre de OpenBSD.
- **IPFilter** ou IPF, pare-feu libre de BSD et Solaris 10.
- **Ipfirewall** ou IPFW, pare-feu libre de FreeBSD.

# Distributions Linux libres

- **Smoothwall**, distribution linux packageant Netfilter et d'autres outils de sécurité pour transformer un PC en pare-feu dédié et complet.
- **IPCop**, distribution linux packageant Netfilter et d'autres outils de sécurité pour transformer un PC en pare-feu dédié et complet.

# logiciels commerciaux

- Check Point FireWall-1, logiciel pare-feu commercial commercialisé par Check Point.
- Seclutions AirLock, pare-feu applicatif commercial.
- NuFW, logiciel pare-feu authentifiant en GPL pour environnement GNU/Linux, client sous licence commerciale pour postes clients Windows
- Pare-feu personnel de Windows XP
- Zone Alarm
- ...

# Pare-feux dédiés

- Il existe un certain nombre de boîtiers combinant souvent pare-feu et routeur
- Cisco Systems
- NetASQ
- Juniper Networks
- ...

# Décisions

- ★ Accepter
- ★ Rejeter
- ★ Supprimer

# Stratégie

- ★ Décision qui s'applique quand aucune règle ne correspond au paquet
- ★ SECURITE : supprimer ce qui n'est pas explicitement autorisé

# Types de flux

## ★ Entrant

- Les paquets à destination des processus internes à la machine

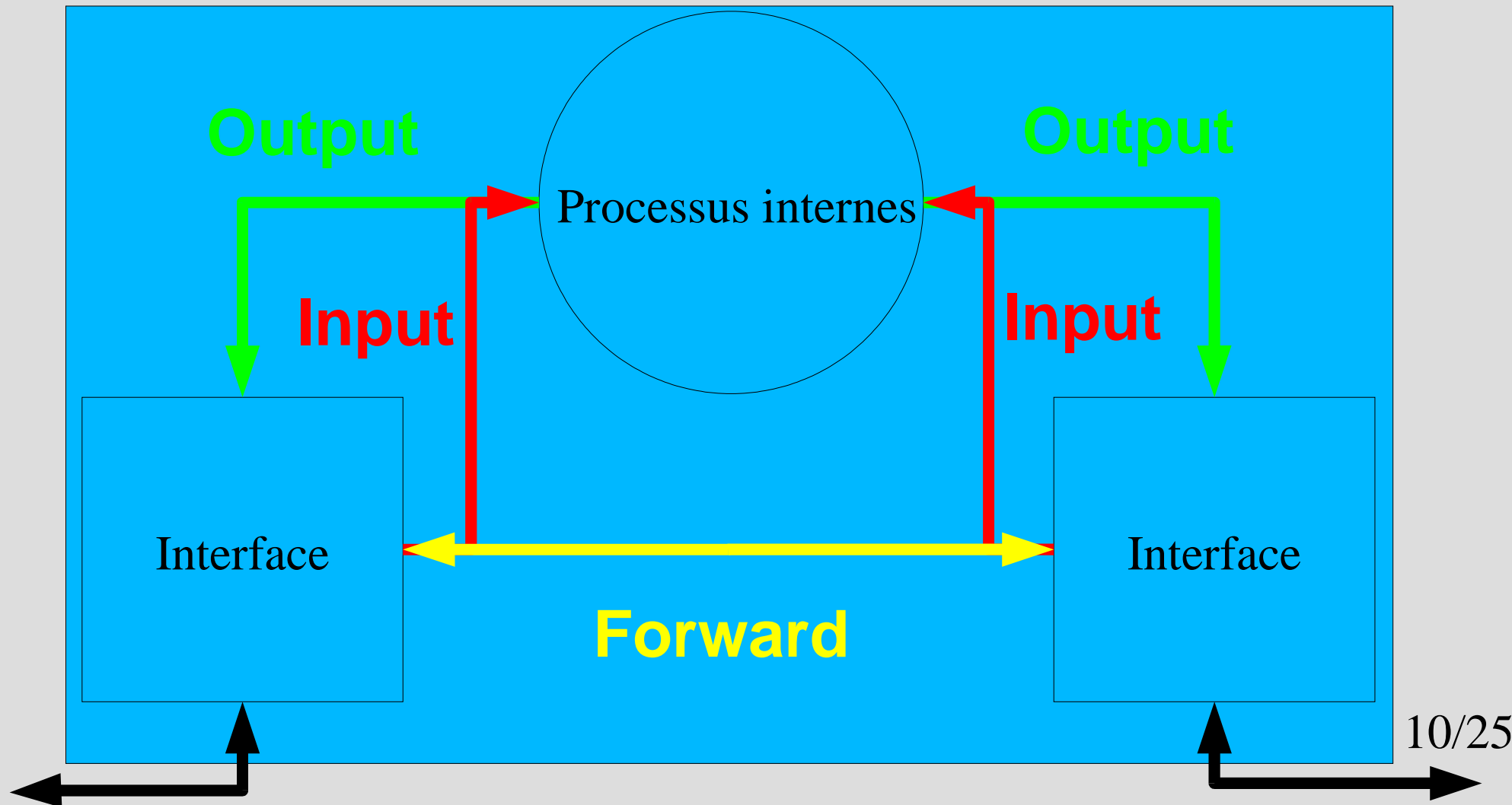
## ★ Sortant

- Les paquets issus des processus internes à la machine

## ★ Transit

- Les paquets qui traversent la machine

# Types de flux



# Exemple

## Vu du pare-feu

Le trafic d'Internet vers le réseau local est :

FORWARD

Le trafic du réseau local vers Internet est :

FORWARD

Une requête « ping request » du réseau local vers le pare-feu est :

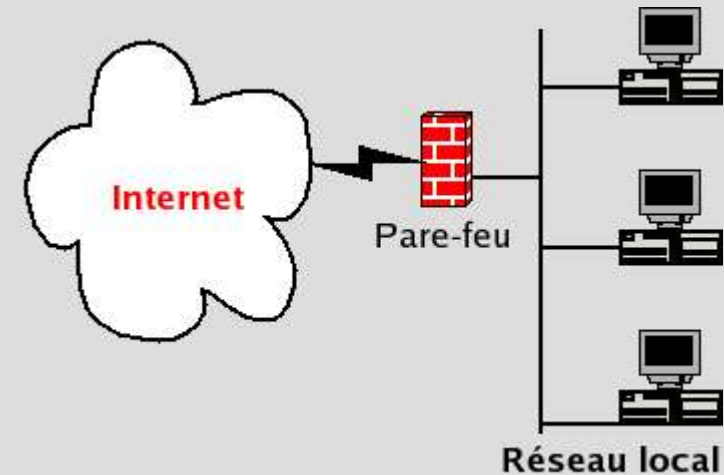
INPUT

Une requête « ping request » d'Internet vers le pare-feu est :

INPUT

La réponse « ping reply » du pare-feu est :

OUTPUT



# Principes de mise en oeuvre

- ★ Exemple avec iptables :
- ★ Effacer toutes les règles existantes
- ★ Définir la stratégie par défaut
- ★ Définir les règles
  - Les règles sont parcourues dans l'ordre. Dès qu'une règle correspond (« match ») on « saute » (-j) vers la chaîne indiquée.
  - Si aucune règle ne correspond on applique la stratégie par défaut

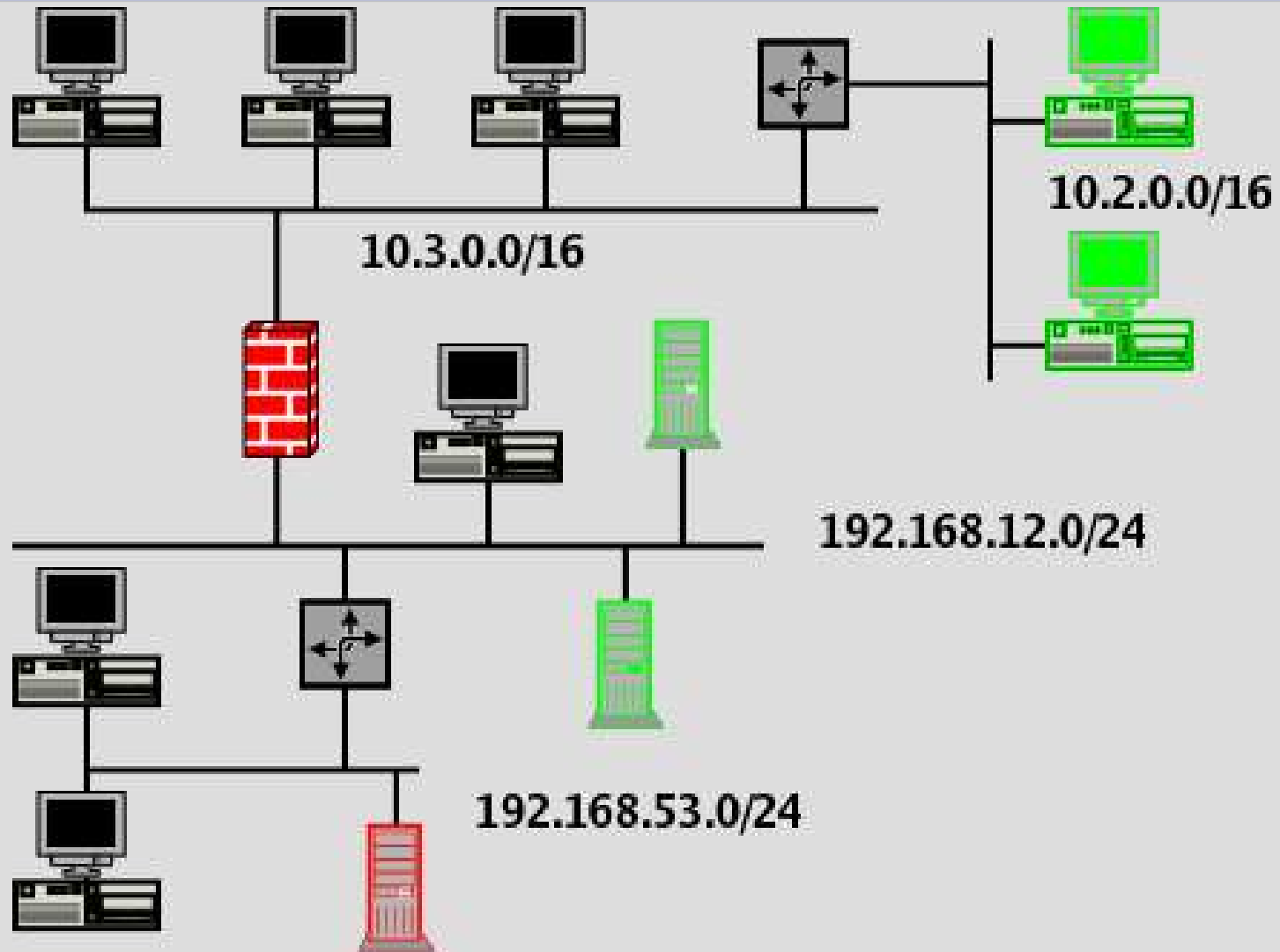
# Dans la vraie vie

- ★ Créez vos règles à la main
- ★ Sauvegardez avec `iptables-save > <mon firewall>`
- ★ Lancez `iptables-restore < <mon firewall>` au démarrage en modifiant  
« `/etc/rc.d/rc.local` »

# Table « filter »

- ★ Chaque paquet passe à travers cette table
- ★ A ajout, D supprime, I insère, F efface toutes les règles mais pas la stratégie par défaut, L liste
- ★ Chaîne INPUT, OUTPUT ou FORWARD
- ★ Critères de sélection du paquet
- ★ Décision

# Exemple



# Example

```
iptables -A FORWARD
```

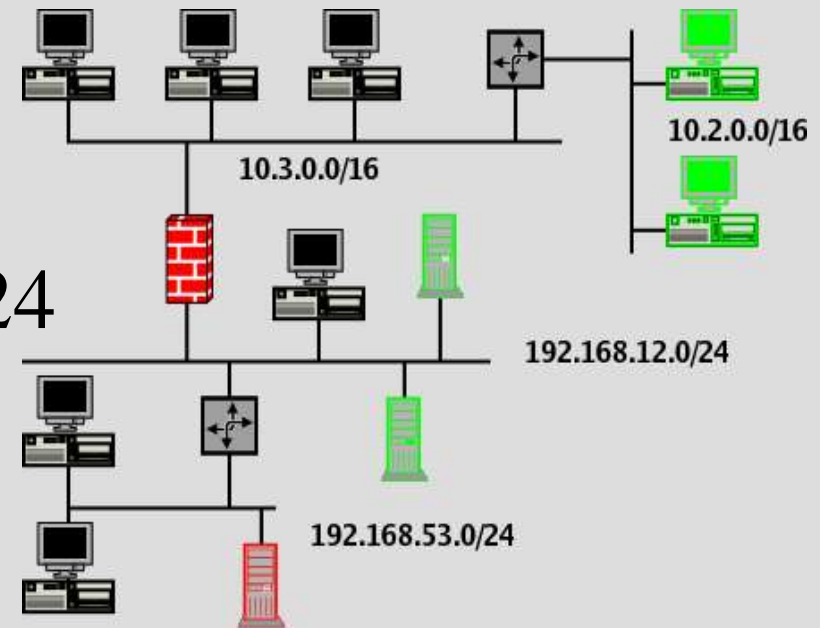
```
-i eth0 -o eth1
```

```
-s 10.2.0.0/16 -d !192.168.12.0/24
```

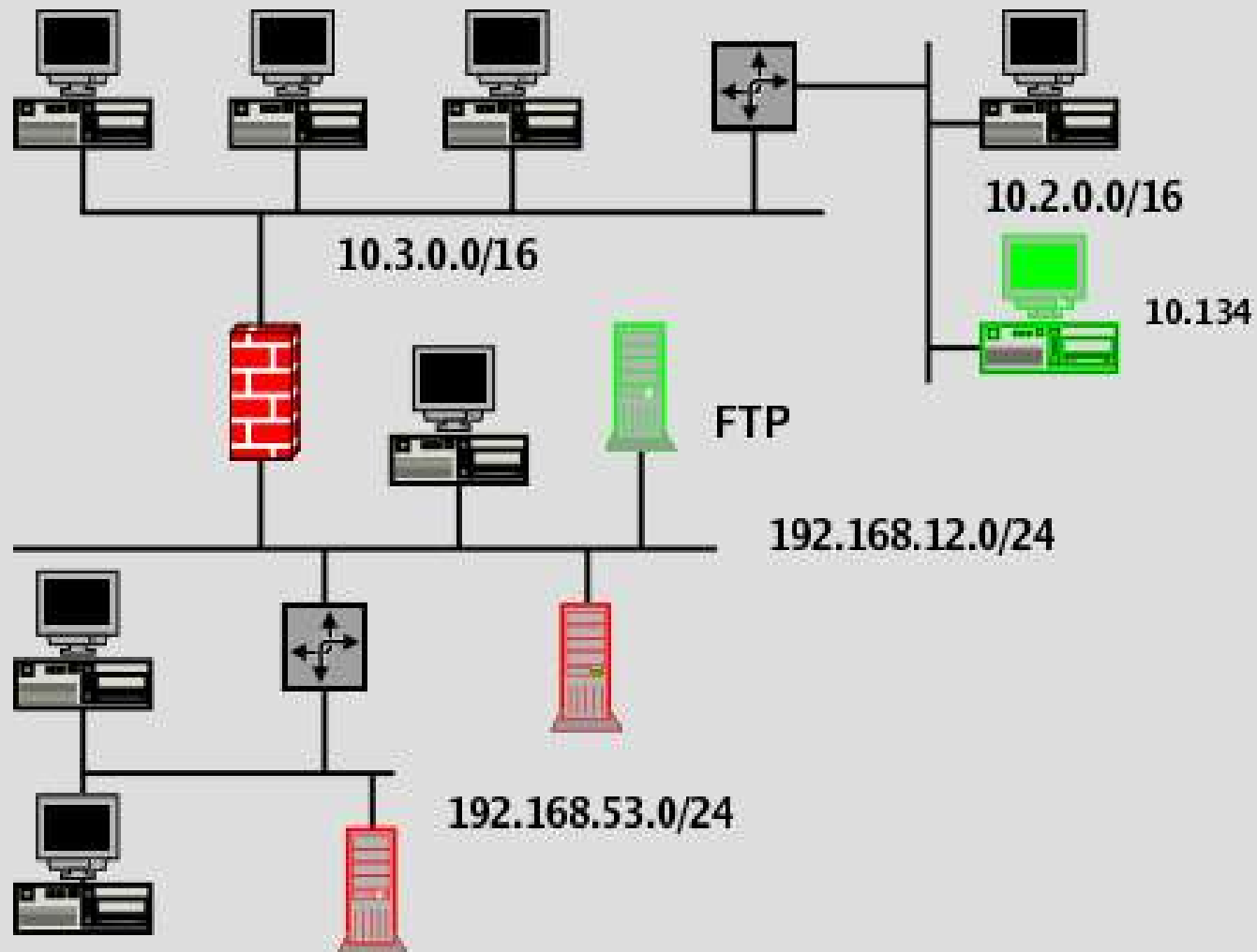
```
-p tcp
```

```
--sport 1024:65535 --dport 80
```

```
-j REJECT --reject-with icmp-host-unreachable
```



# Etats

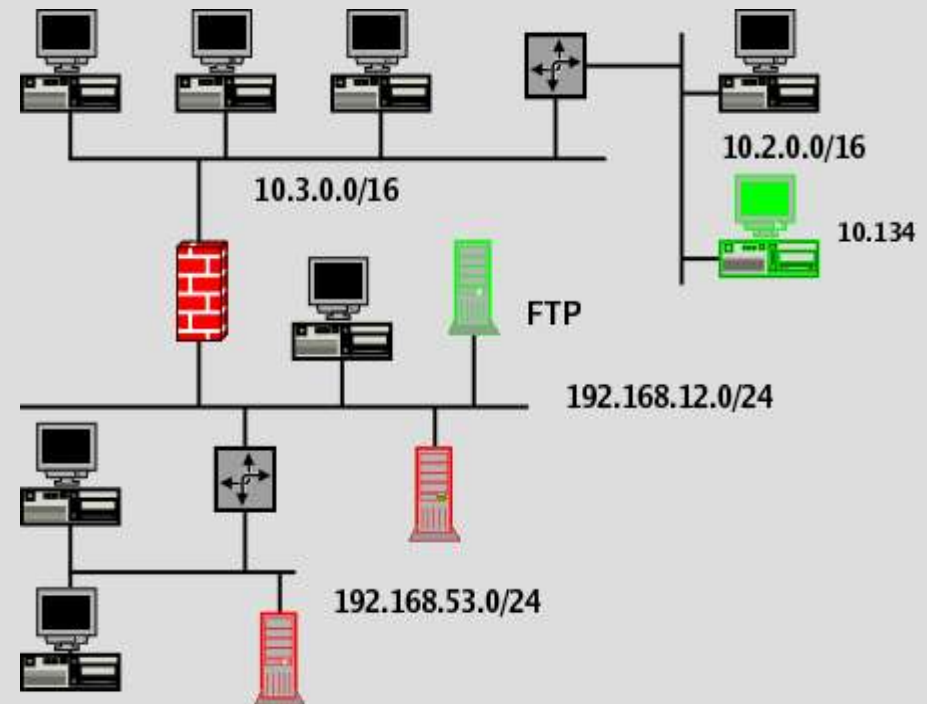


# Etats

```
iptables -A FORWARD  
-i eth0 -o eth1  
-s 10.2.10.134 -d 192.168.12.65  
-p tcp  
--sport 1024:65535 --dport 21  
--state NEW,ESTABLISHED  
-j ACCEPT
```

---

```
iptables -A FORWARD -i eth0 -o eth1 -s 10.2.10.134 -d  
192.168.12.65 -p tcp --state ESTABLISHED, RELATED -j  
ACCEPT
```



# Translation d'adresse

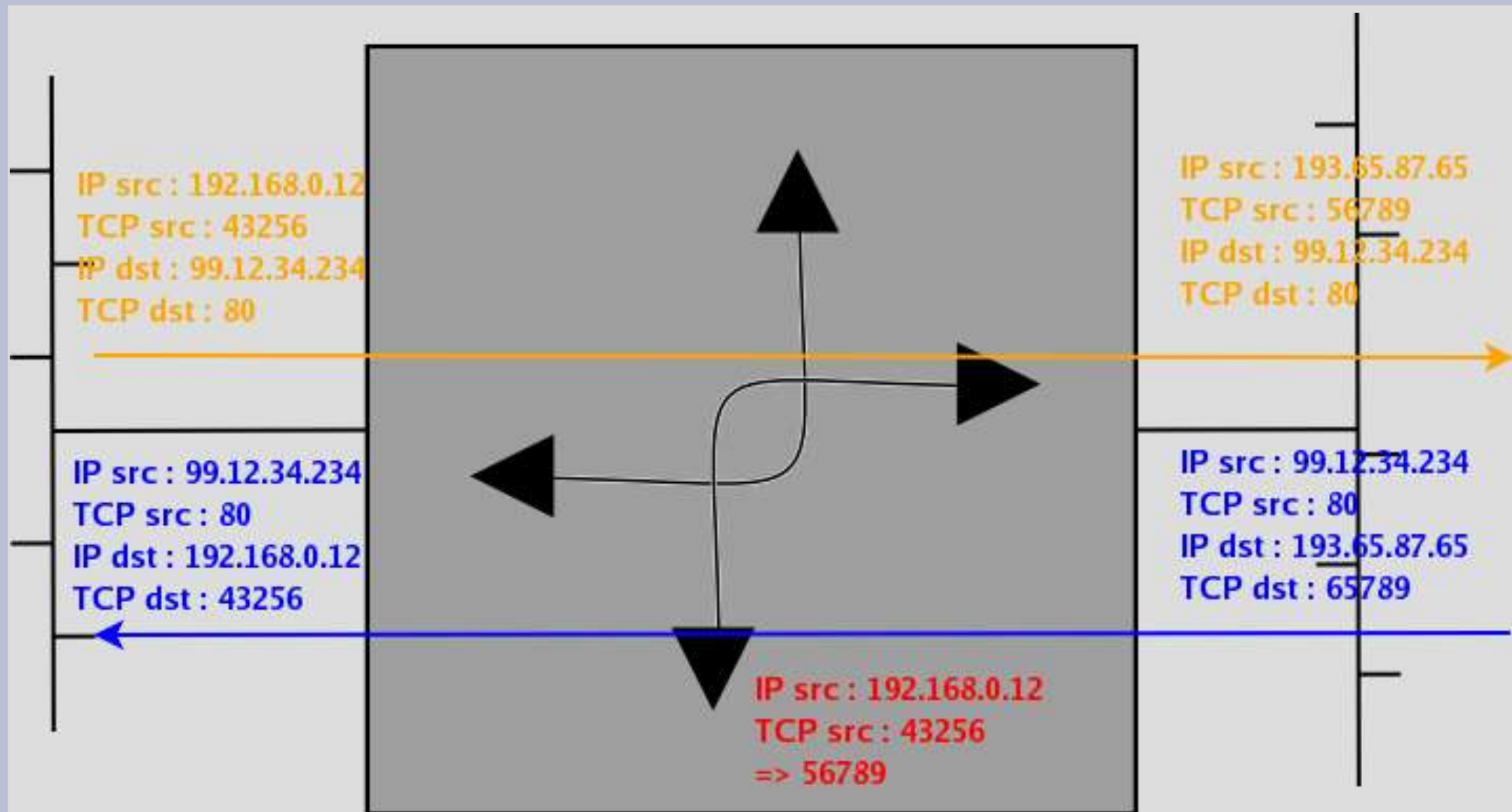
## ★ Paquets sortants :

- remplacement de l'adresse IP source
- remplacement du port tcp/udp source

## ★ Paquets entrants :

- remplacement de l'adresse IP destination
- remplacement du port tcp/udp

# Masquerading



# Table « NAT »

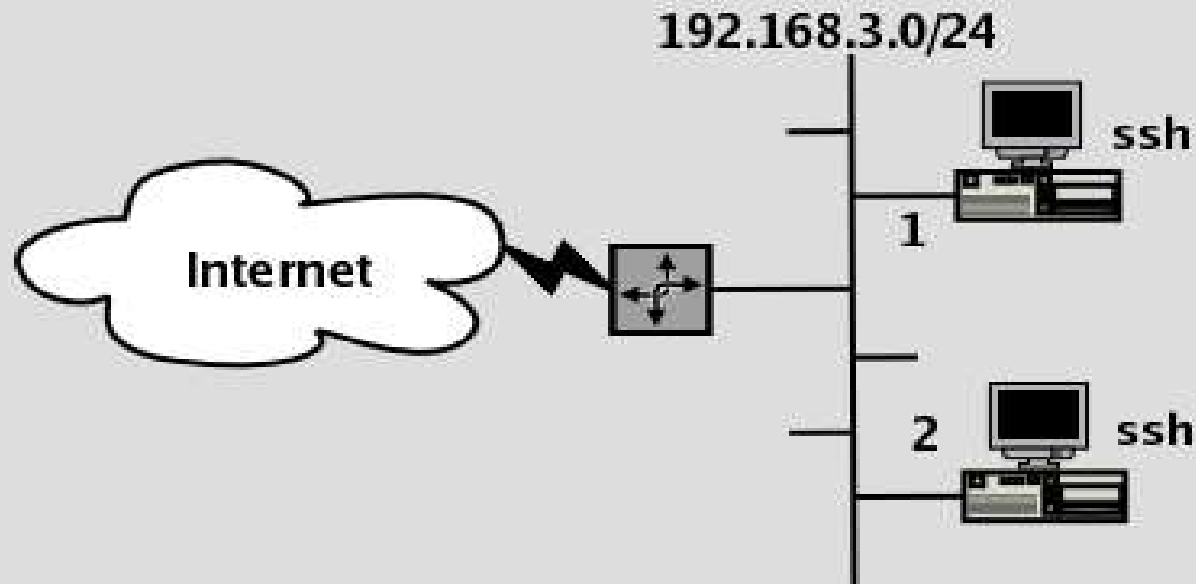
- ★ Permet la translation d'adresses
- ★ Le premier paquet de chaque connexion passe à travers cette table
- ★ 3 chaînes prédéfinies :
  - PREROUTING : l'adresse de destination est modifiée pour les paquets entrants AVANT la décision de routage
  - POSTROUTING : l'adresse source est modifiée pour les paquets sortants APRES la décision de routage
  - OUTPUT translation d'adresses de destination uniquement pour les paquets créés par cet ordinateur

# NAT source

- ★ Modification APRES la décision de routage
- ★ Spécifier les interfaces d'entrée et de sortie
- ★ Cas particulier du camouflagement  
« masquerading »

```
iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

# NAT destination



- ★ `iptables -t nat -A PREROUTING -p tcp --dport 22 -i eth0 -j DNAT --to 192.168.3.1:22`
- ★ `iptables -t nat -A PREROUTING -p tcp --dport 2222 -i eth0 -j DNAT --to 192.168.3.2:22`

# Table « mangle »

- ★ transformation des options des paquets, comme la régulation de la bande passante, très utile pour lutter contre les attaques en « DOS »

# Interfaces graphiques

- ★ Il existe des interfaces graphiques permettant de créer les règles iptables
  - Soit c'est aussi complexe qu'en ligne de commande
  - Soit on ne sait pas ce qu'on fait
- ★ On ne construit pas un firewall tous les jours !
- ★ Un firewall c'est compliqué !!!