Exemple de configuration d'un firewall sous Linux

Alain Knaff
alain.knaff@lll.lu

Buts

- Protéger le réseau interne
- Multiplexage de plusieurs machines sur une même addresse IP publique unique
  - Permet d’accéder à Internet depuis plusieurs stations de travail
  - Aiguillage de requêtes entrantes sur plusieurs serveurs

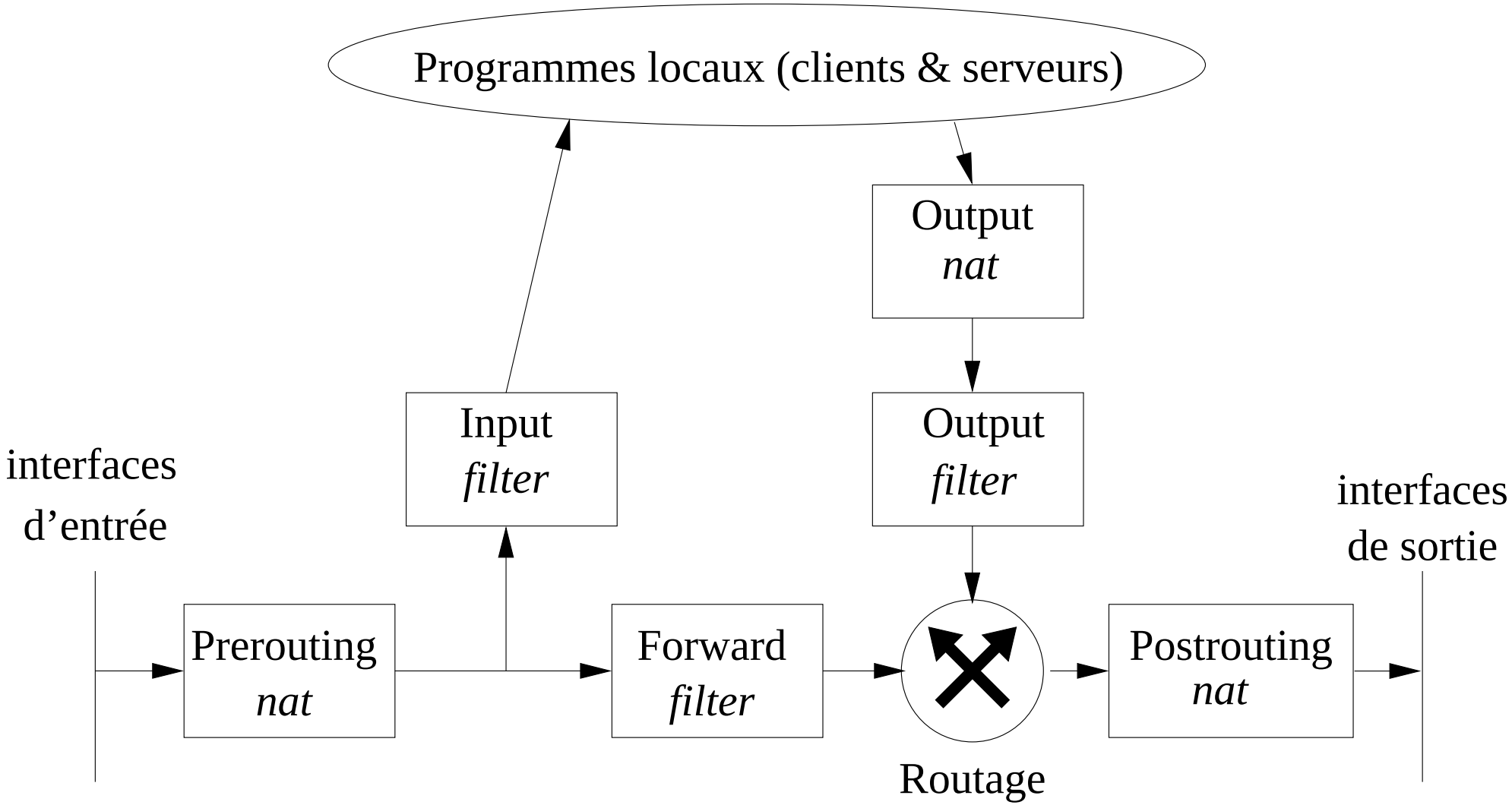
Cadre

- Firewall basé sur le *filtrage de paquets*
- API Iptables (noyau 2.4)

Concepts

- Tables: `filter` (par défaut), `nat`, `mangle`
- Chaînes: `INPUT`, `OUTPUT`, `FORWARD`, `PREROUTING`, `POSTROUTING`
- Règles

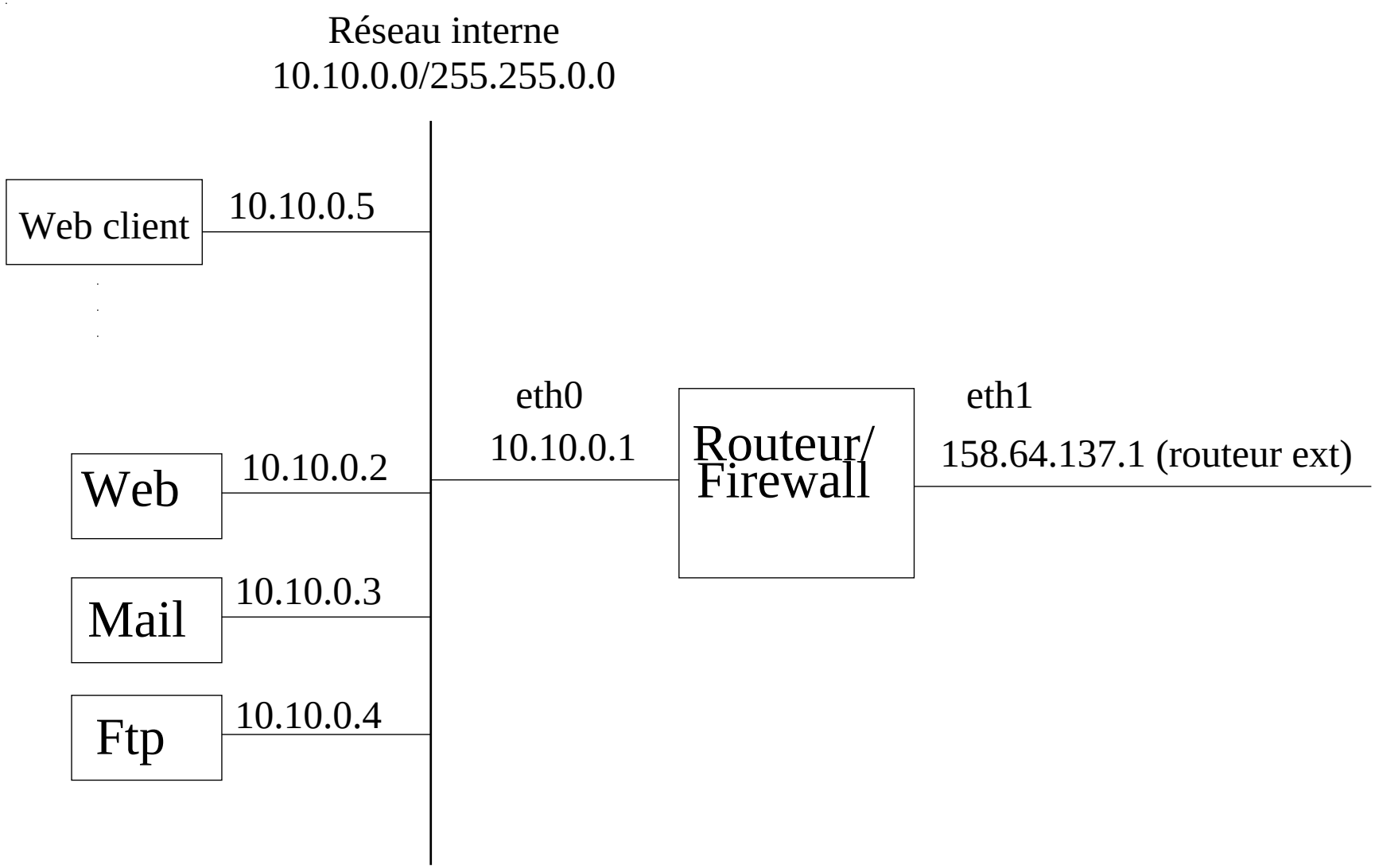
Flux des paquets



Syntaxe de la commande

- Syntaxe: `iptables [table] chainspec condition action`
- Actions:
  - -A *chaîne* rajouter à la fin
  - -I *chaîne* insérer au début
  - -D *chaîne* supprimer la règle
  - -F *chaîne* supprimer toutes les règles
- Exemples:
  - ```
    iptables  -t nat -A OUTPUT -d 10.10.1.1 \
     -j DNAT --to-destination 1.2.3.4
    ```
  - ```
    iptables -A FORWARD -d 10.10.1.1 -j DROP
    ```

Diagramme réseau



Protection du réseau interne

- Interdire accès depuis l’extérieur (eth1)
- Autoriser accès ssh (administratif)
- Autoriser voie de retour

```
iptables -A INPUT -i eth1 -j DROP
iptables -I INPUT -p tcp --dport 22 -j ACCEPT
iptables -I INPUT -m state --state ESTABLISHED -j ACCEPT
```

Nat sortante (Accès Web)

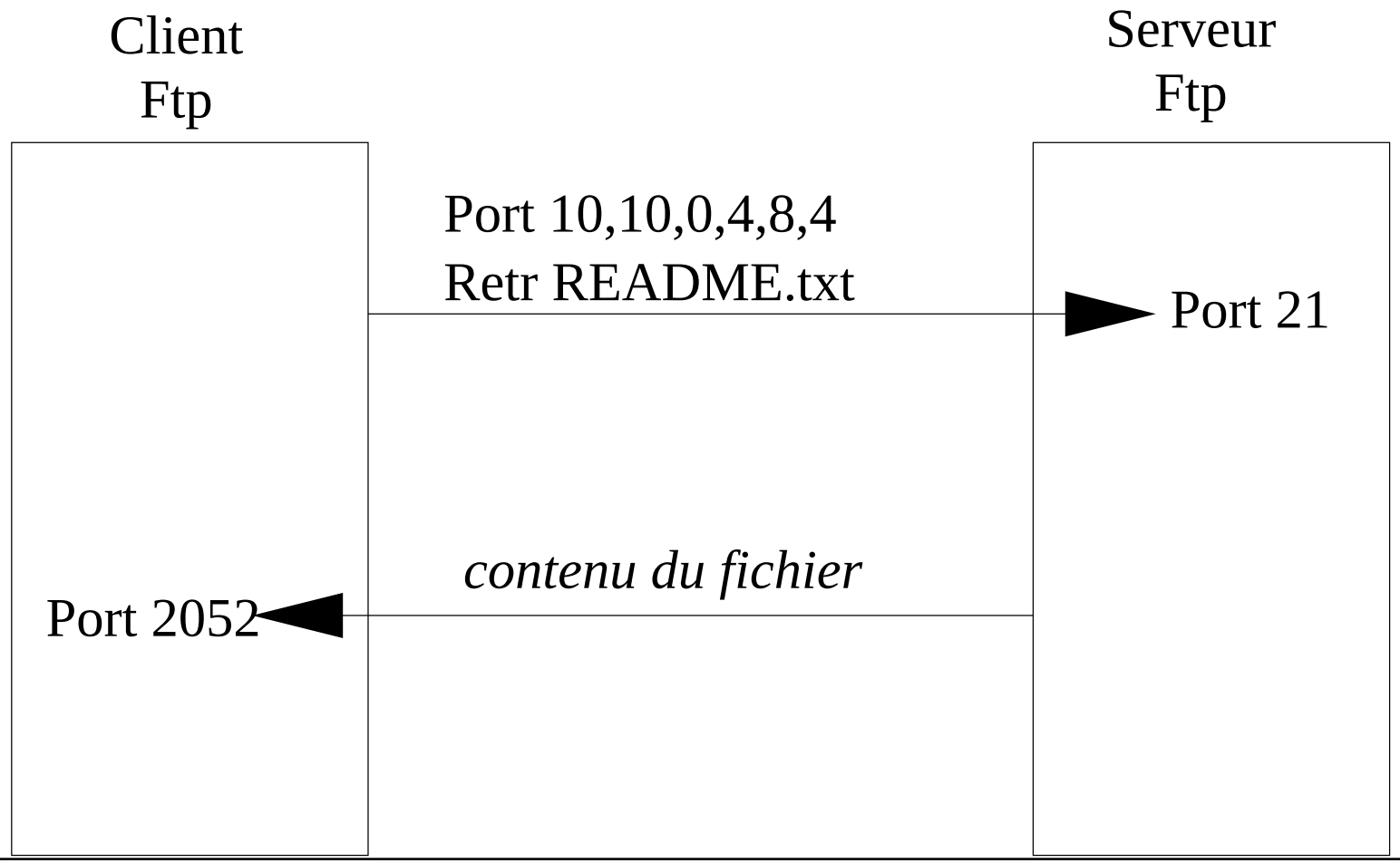
- Les machines intérieures vont utiliser l'addresse du routeur

```
iptables -t nat -A POSTROUTING -s 10.10.0.0/16 \
 -j SNAT ---to-source 158.64.137.1
```

- Si le routeur a une addresse IP variable, utiliser l'option -j MASQ au lieu de -j DNAT

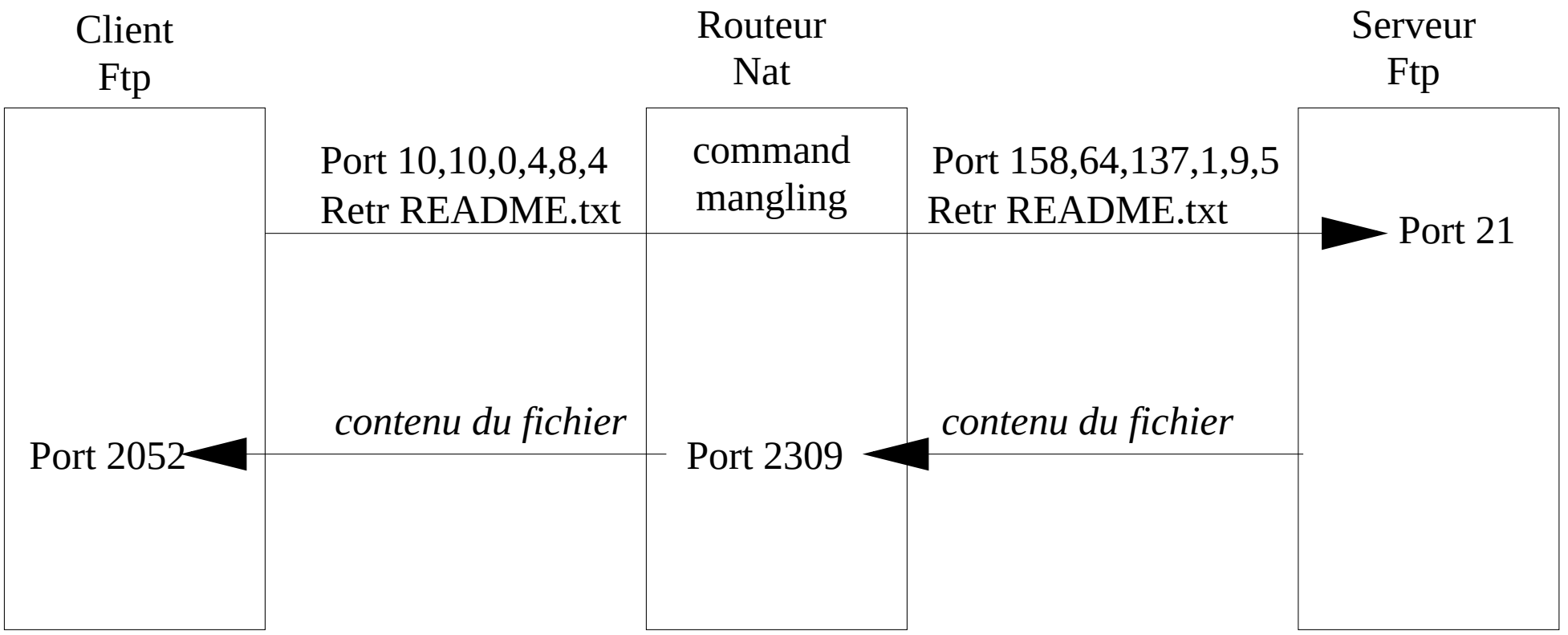
Transfer FTP, sans NAT

- En mode passif, le serveur rappelle le client sur un port que le client spécifie



Transfer FTP, avec NAT

- Le routeur NAT remplace l'addresse de rappel dans la connection de contrôle



Mise en place de la NAT Ftp:

```
modprobe ip_nat_ftp
modprobe ip_conntrack_ftp
```

Nat entrante

- Aiguillage des requêtes entrantes sur les bonnes machines

```
iptables -t nat -I PREROUTING \
 -p tcp -d 158.64.137.1 --dport 80 \
 -j DNAT --to-destination 10.10.0.2
```

- Autorisation de l’accès

```
iptables -I FORWARD \
 -p tcp -d 10.10.0.2 --dport 80 \
 -j ACCEPT
```

Proxy transparent, configuration NAT

- Le routeur NAT intercepte toutes les connections destiné es aux serveurs Web externes, et les passe au processus Squid local

```
iptables -t nat -I PREROUTING \
 -p tcp --dport 80 -i eth0 \
 -j DNAT --to-destination 10.10.0.1:3128
```

Proxy transparent, configuration Squid

- Le proxy squid doit être préparé à accepter ces requêtes interceptées:

```
httpd_accel_uses_host_header on
httpd_accel_with_proxy on
httpd_accel_host virtual
```

Urls de cette présentation

- Cette présentation sera placée à l'URL suivante:

`http://www.lll.lu/firewall-presentation/fw.pdf`

- Un script exemple se trouve ici:

`http://www.lll.lu/firewall-presentation/fw.sh`

- Il existe de nombreux outils "graphiques" et distributions "ad-hoc" pour gérer un firewall. Exemple: Ipcop:

`http://www.ipcop.org/`

Questions?