Firewall, DMZ, et ACL

2021/ 2022

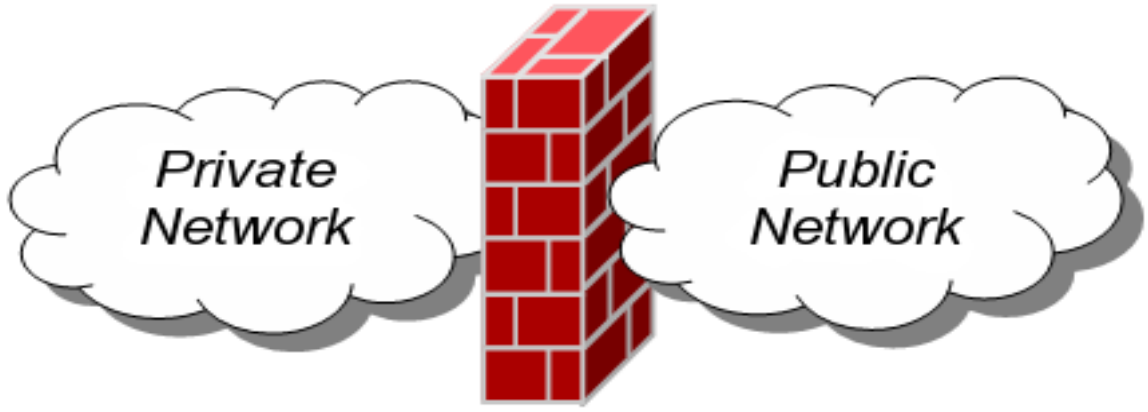
Pourquoi utiliser un firewall

Definition

Programme, ou un matériel, chargé de vous protéger du monde extérieur en contrôlant tout ce qui passe, et surtout tout ce qui ne doit pas passer entre internet et le réseau local.

pourquoi un firewall?

- Contrôle. Gérer les connexions sortantes a partir du réseau local.
- Sécurité. Protéger le réseau interne des intrusions venant de l'extérieur.
- Vigilance. Surveiller/tracer le trafic entre le réseau local et internet.



Plusieurs types de firewalls :

* Pare-feu au niveau réseau
* Pare-feu au niveau applicatif
* Pare-feu des applications

Différents types de firewalls

Pare-feu niveau réseau. (iptables, paquet filter, . . .)

- Firewall fonctionnant à un niveau bas de la pile TCP/IP
- Basé sur le filtrage des paquets
- Possibilité (si mécanisme disponible) de filtrer les paquets suivant l'état de la connexion

Intérêt : Transparence pour les utilisateurs du réseau

Pare-feu au niveau applicatif. (inetd, xinetd, . . .)

- Firewall fonctionnant au niveau le plus haut de la pile TCP/IP
- Généralement basé sur des mécanisme de proxy

Intérêt : Possibilité d'interpréter le contenu du trafic

Pare-feu des applications. (/etc/ftpaccess pour ftp, . . .)

- Restrictions au niveau des différentes applications

DMZ

Definition (DMZ)

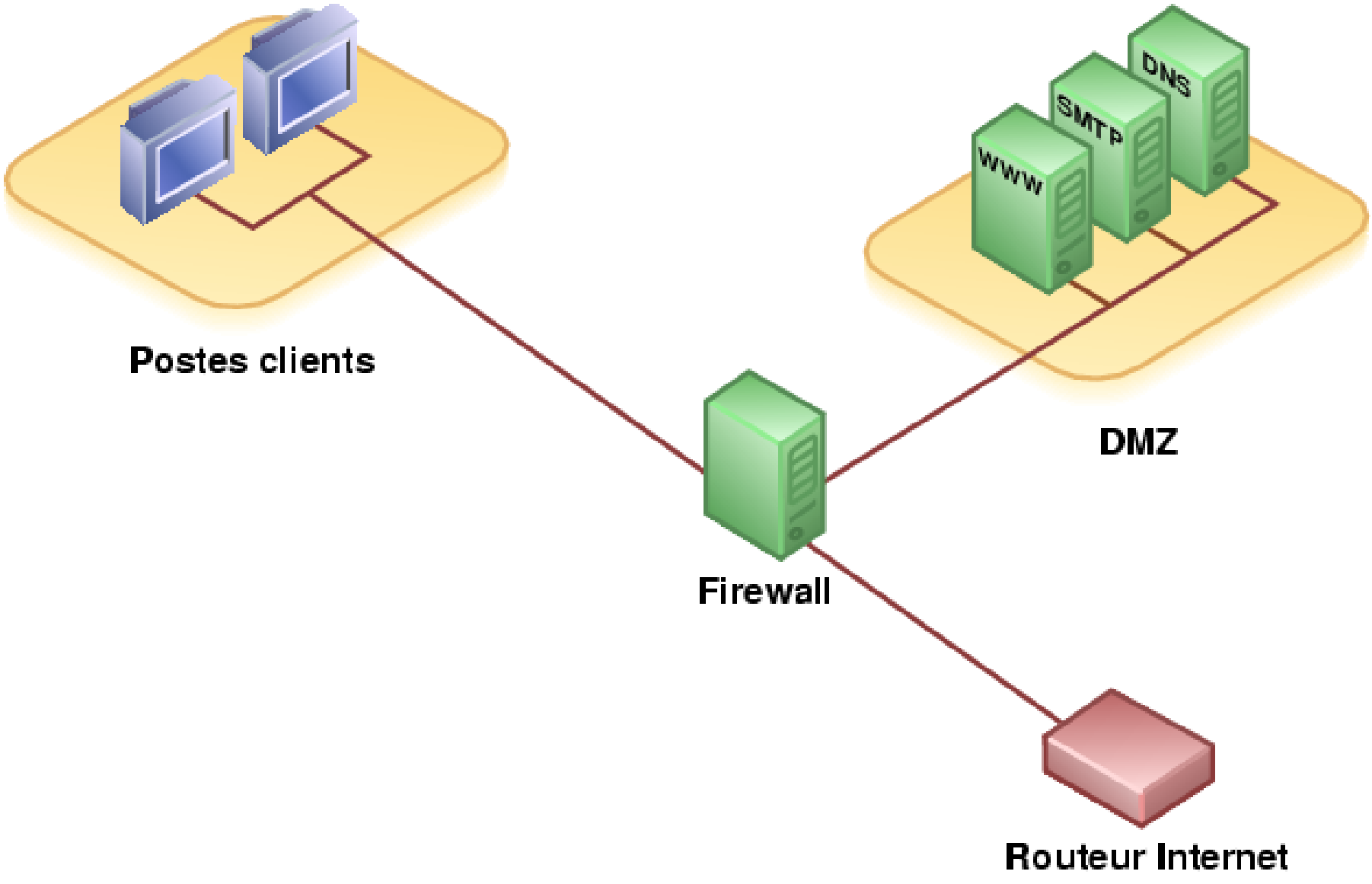
Une zone démilitarisée (DMZ) est un sous-réseau se trouvant entre le réseau local et le réseau extérieur.

Propriétés :

* Les connexions à la DMZ sont autorisées de n'importe où.
* Les connexions à partir de la DMZ ne sont autorisées que vers l'extérieur.

Intérêt :

* Rendre des machines accessible à partir de l'extérieur (possibilité de mettre en place des serveurs (DNS, SMTP, . . .).


Postes clients
WWW
SMTP
DNS
DMZ
Firewall
Routeur Internet

Iptables et filtrage(1/2)

- Filtrage des paquets IP, TCP, UDP ou ICMP
- Spécification de règle pour le rejet ou l'acceptation de paquet
- Utilisation de la table FILTER et des chaînes INPUT, OUTPUT et FORWARD
- Règles traitées de manière séquentielle : Le paquet sort dès qu'il rencontre une règle qui peut lui être appliquée

Exemples :

- Accepter tous les paquets en provenance de n'importe où et destinés à l'adresse du routeur 192.168.1.1.

```
iptables -A INPUT -s 0/0 -i eth0 -d 192.168.1.1 -p TCP
-j ACCEPT
```

- Accepter de router les paquets entrant sur eth0 tels que :

@source	@dest	P-source	P-dest
0/0	192.168.1.58	1024-65535	80

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o
eth1 -p TCP --sport 1024:65535 --dport 80 -j ACCEPT
```

Iptables et filtrage(2/2)

- Accepter un paquet ICMP “echo-request” (ping) par seconde

```
iptables -A INPUT -p icmp --icmp-type echo-request -m limit --limit 1/s -i eth0 -j ACCEPT
```

- Accepter 5 segments TCP ayant le bit SYN positionné par seconde (permet d’éviter de se faire inonder)

```
iptables -A INPUT -p tcp --syn -m limit --limit 5/s -i eth0 -j ACCEPT
```

- Accepter de router les paquets entrants sur eth0 tels que :

@source	@dest	P-source	P-dest
0/0	192.168.1.58	1024-65535	80 ou 443

```
iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p TCP --sport 1024:65535 -m multiport --dport 80,443 -j ACCEPT
```

Iptables et suivi des connexions

* Suivi des connexions disponible (*conntrack*)
* Quatre états possibles pour une connexion :
  - NEW . Nouvelle connexion établie
  - ESTABLISHED . La connexion analysée est déjà établie
  - RELATED . La connexion est en relation avec une connexion déjà établie (ftp-data par exemple)
  - INVALID . Le paquet reçu n'appartient à aucune des trois catégories précédentes.

Exemples :

* Autoriser tous les paquets émis par le routeur concernant des connexions déjà établies.

```
iptables -A OUTPUT -o eth0 -m state --state
ESTABLISHED,RELATED -j ACCEPT
```

Iptables et suivi des connexions

* Suivi des connexions disponible (*conntrack*)
* Quatre états possibles pour une connexion : NEW . Nouvelle connexion établie

ESTABLISHED . La connexion analysée est déjà établie

RELATED . La connexion est en relation avec une connexion déjà établie (ftp-data par exemple)

INVALID . Le paquet reçu n'appartient à aucune des trois catégories précédentes.

Exemples :

* Autoriser le routeur à relayer tous les paquets reçus concernant de nouvelles connexions sur le port 22. `iptables -A FORWARD -p tcp -i eth0 --dport 22 --sport 1024:65535 -m state --state NEW -j ACCEPT`

Outils de diagnostic

Traces iptables. Possibilité de tracer certaines actions iptables.

exemple :

1. Tracer toutes les actions iptables :

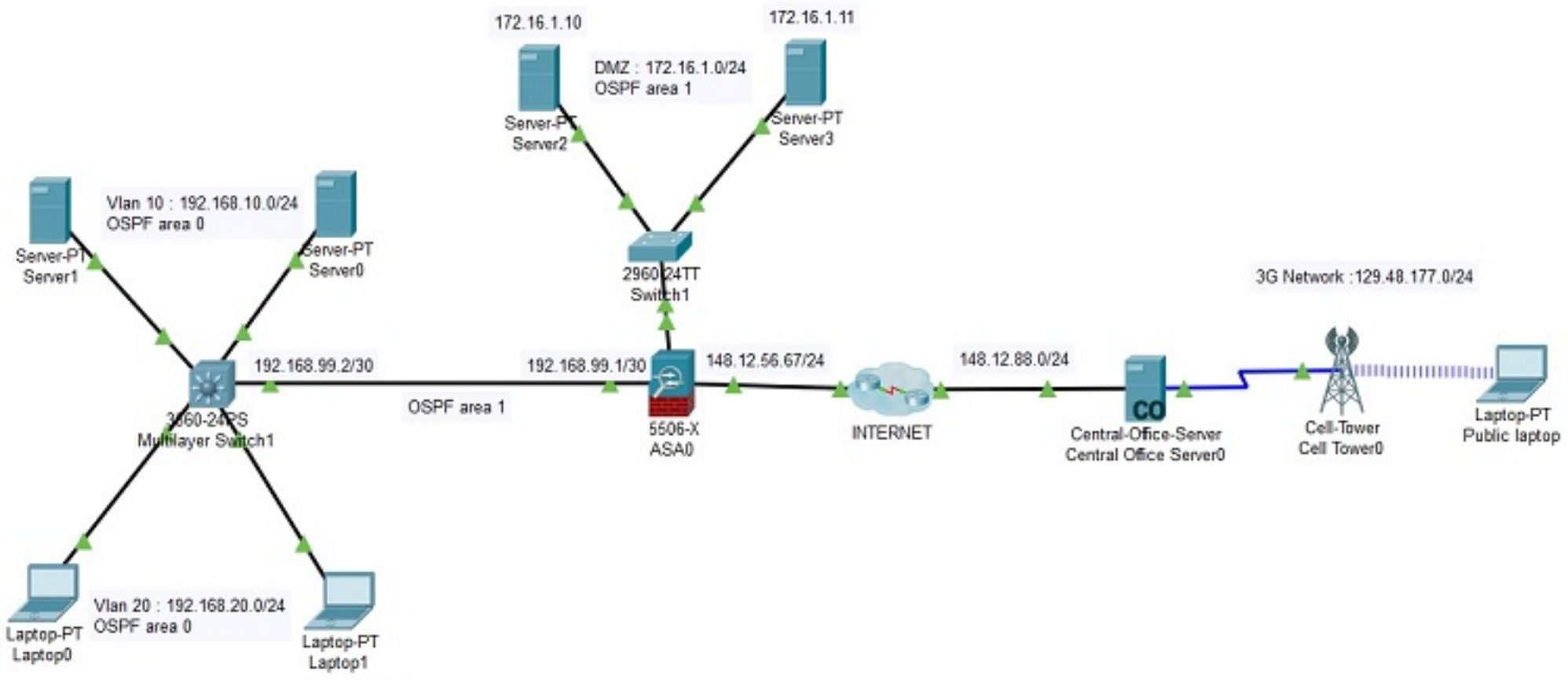
```
iptables -A OUTPUT -j LOG
iptables -A INPUT -j LOG
iptables -A FORWARD -j LOG
```

2. Rajouter une règle pour tracer les paquets rejetés

```
iptables -N LOG_DROP
iptables -A LOG_DROP -j LOG --log-prefix
'[IPTABLES DROP] : '
iptables -A LOG_DROP -j DROP
```

nmap, nessus,. . . . Logiciels permettant de diagnostiquer l'état d'un firewall (trouver les ports ouverts, détecter les services utilisant les ports, . . .)

TP Packet Tracer lab 18 : ASA 5506-X DMZ configuration



1. Configurez NAT pour permettre aux utilisateurs LAN d'accéder à INTERNET
2. Configurez NAT pour permettre aux serveurs DMZ d'accéder à INTERNET
3. Configurez la règle NAT entrante pour autoriser l'accès au serveur Web 172.16.1.10 DMZ à partir d'Internet avec l'adresse IP publique 148.12.56.68.
4. Configurez les règles ICMP pour permettre à laptop1 d'envoyer un ping au routeur Internet 148.12.56.1 et à toute ressource Internet. Une liste d'accès, nommée OUTSIDE, sera configurée pour autoriser les réponses d'écho entrantes et les réponses ICMP inaccessibles.
6. Testez la connectivité HTTP de l'ordinateur portable public au serveur Web DMZ (http://148.12.56.68)

ACL

C’est quoi le ACL?

- *Access Control List*（ACL）
  - Liste de contrôle d’accès， Conditions appliquées au trafic circulant via une interface d’un routeur
  - Indiquer au routeur les types de paquets à accepter ou à rejeter en fonction de conditions précises
  - Permet de gérer le trafic et de sécuriser l’accès d’un réseau en entrée comme en sortie

- Principe fonctionnement de ACL
  - analyser les informations de l’entête paquets de couches 3 et 4
  - faire le filtrage d’après les règles pré-défis

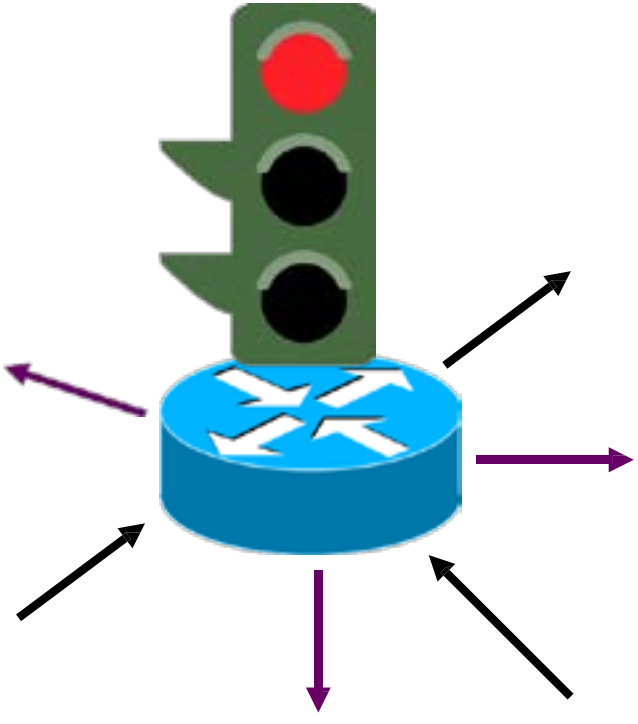
Motivation & Rôle 2-1

- Fournir un niveau de sécurité d'accès réseau de base
- Appliquer dans QoS

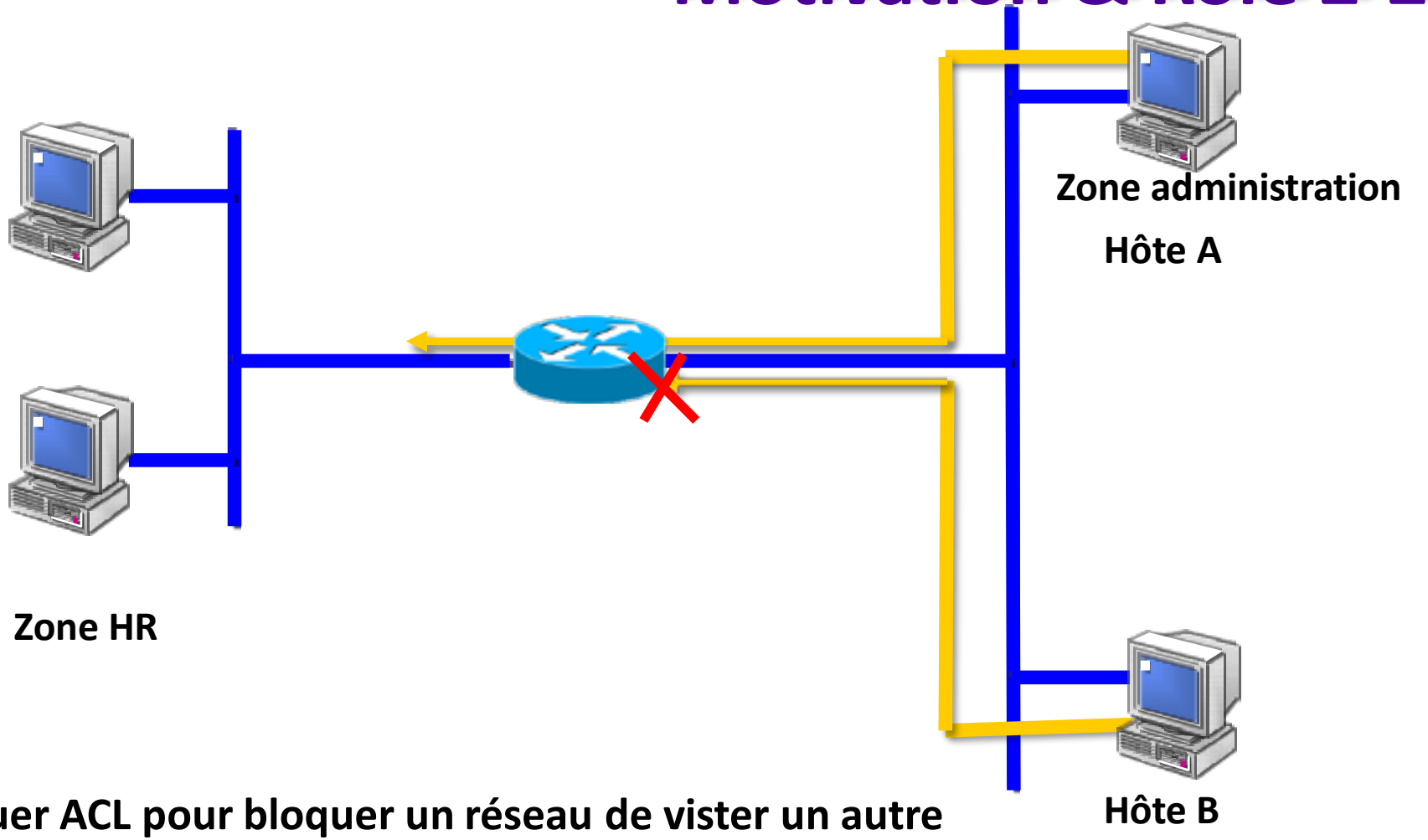
pour contrôler le flux de trafic

- Limiter le trafic réseau et

Accroître les performances



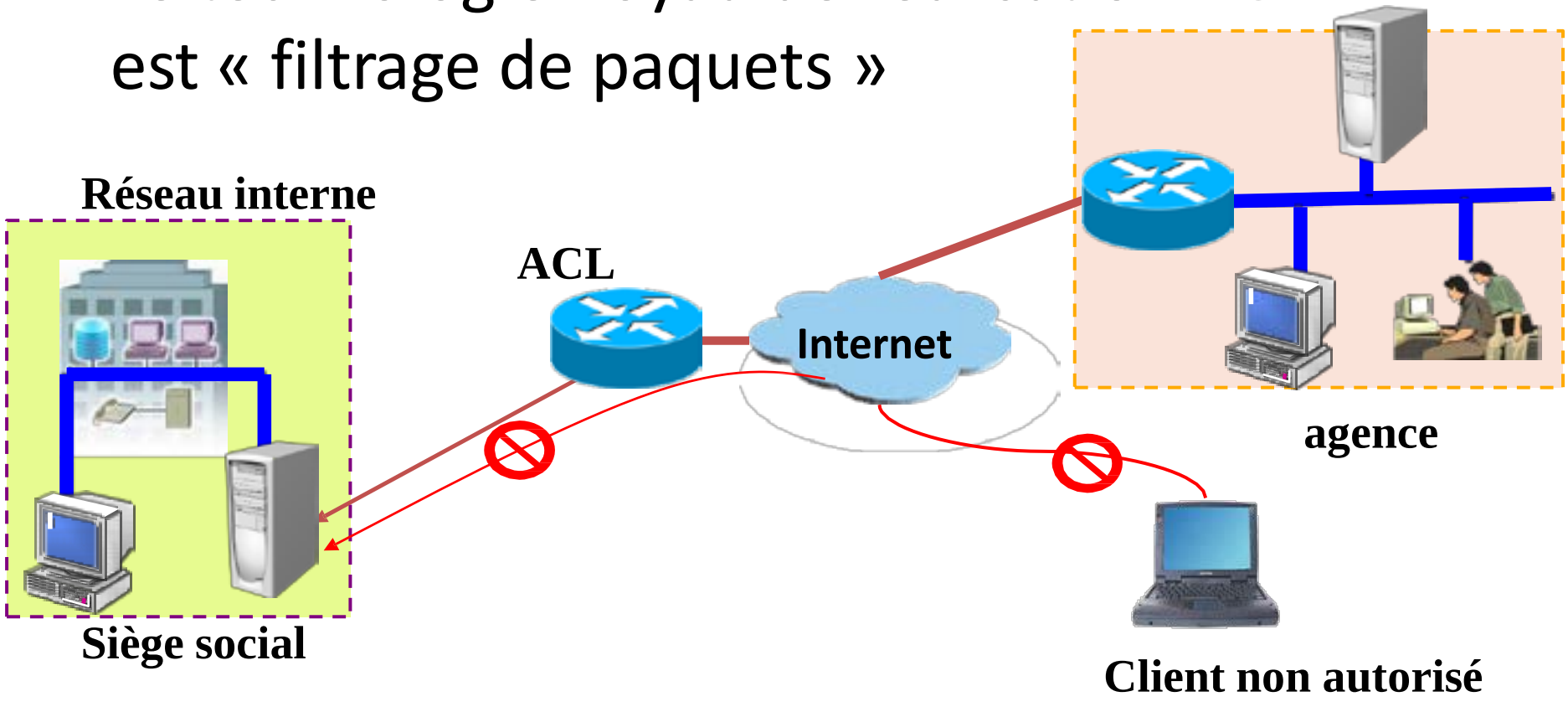
Motivation & Rôle 2-2



Appliquer ACL pour bloquer un réseau de vister un autre

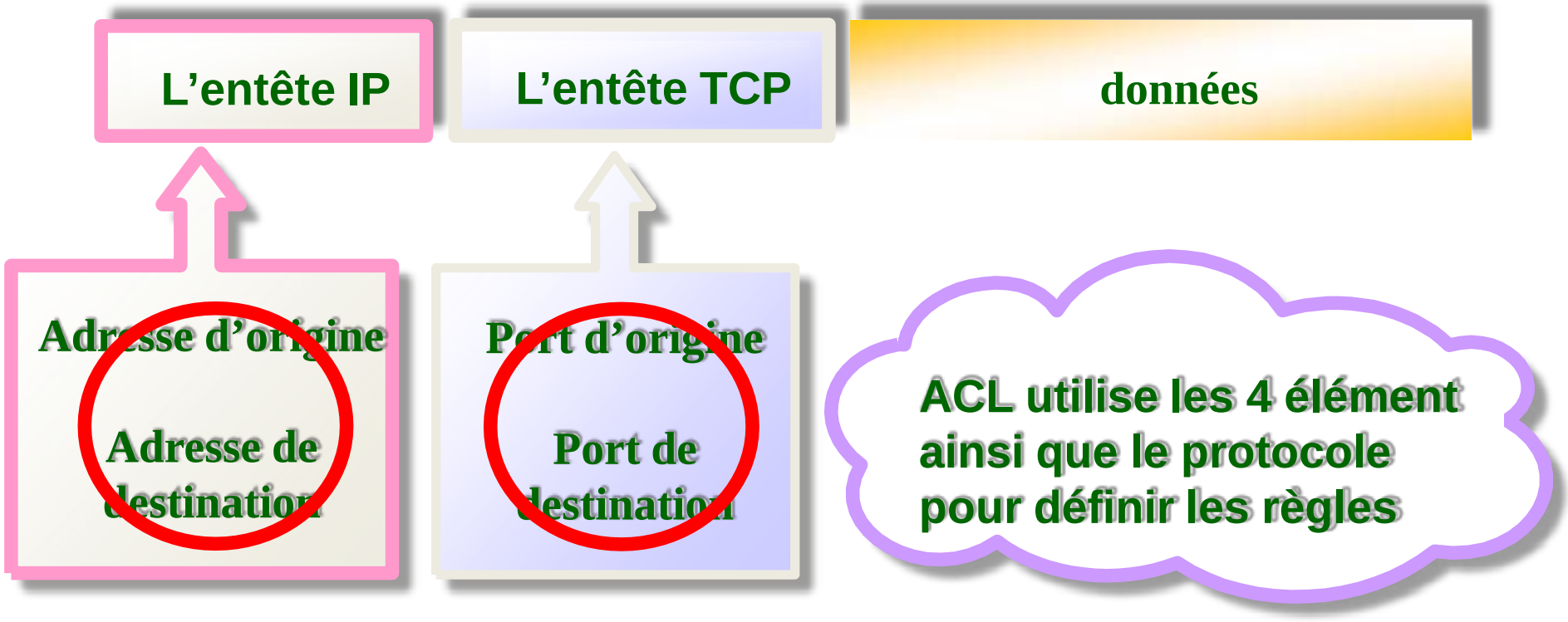
Fonctionnement 2-1

- Le technologie noyau de réalisation ACL est « filtrage de paquets »



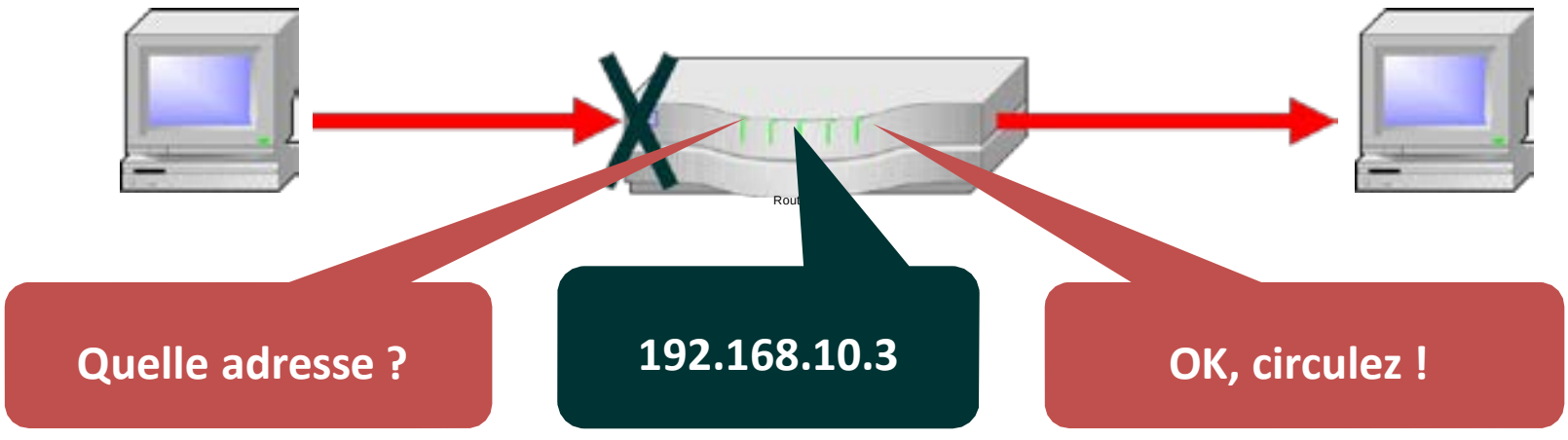
Fonctionnement 2-2

- Le routeur examine chaque paquet afin de déterminer s'il doit l'acheminer ou le rejeter en fonction des conditions précisées dans la liste de contrôle d'accès.
- Certaines conditions dans une ACL sont des adresses source et de destination, des protocoles et des numéros de port de couche supérieure.



ACL - Comment ça marche 2-1

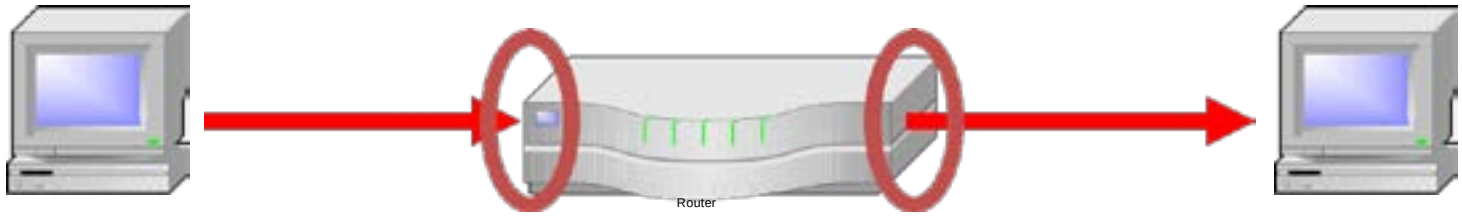
- Filtre les paquets en utilisant des éléments des couches 3 (adresses IP) et 4 (numéros de port des applications) de TCP-IP ;
- Par défaut, une liste de contrôle non paramétrée refuse tous les accès.



- Le paramétrage de l'ACL décide quel hôte ou groupe d'hôte peut (permit) ou ne peut pas (deny) transiter par le routeur.

ACL - Comment ça marche 2-2

- Les ACLs sont créées en mode de configuration globale.
- Elles doivent ensuite être affectée à un (ou plusieurs) ports.

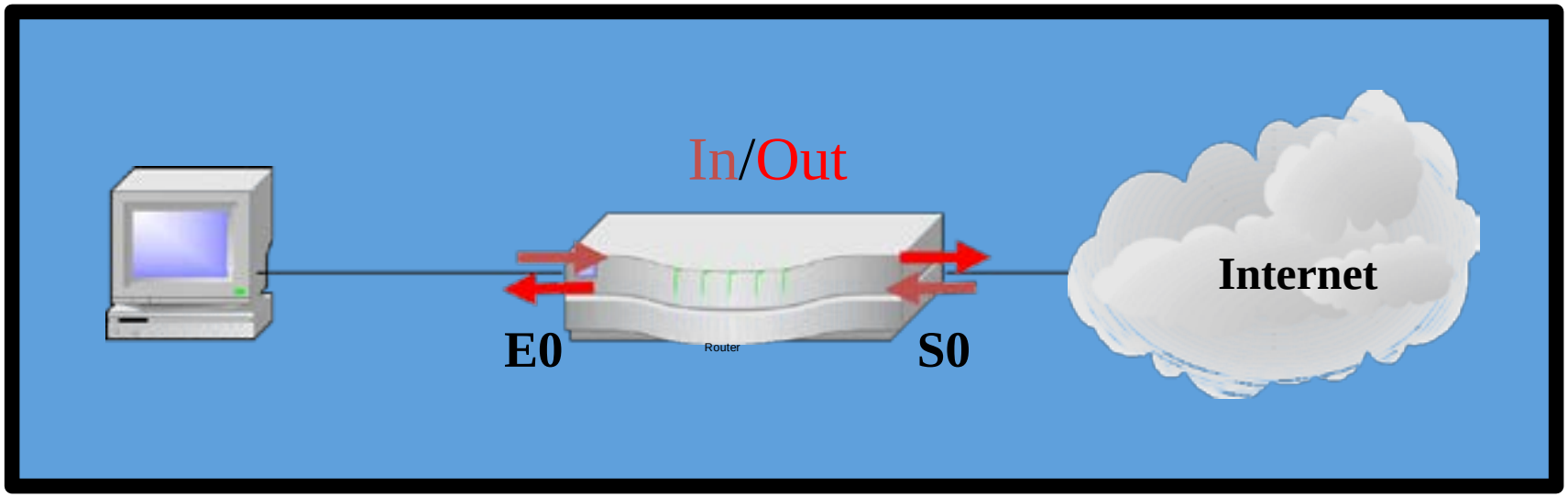


- Grâce aux *masques génériques (wildcard mask)*, le contrôle peut s'appliquer à un réseau, un sous-réseau, un hôte ou une catégorie d'hôtes.
- Ne contrôle pas les paquets émis par le routeur lui-même.

Les paramètres *In* et *Out*

(Inbound-Outbound)

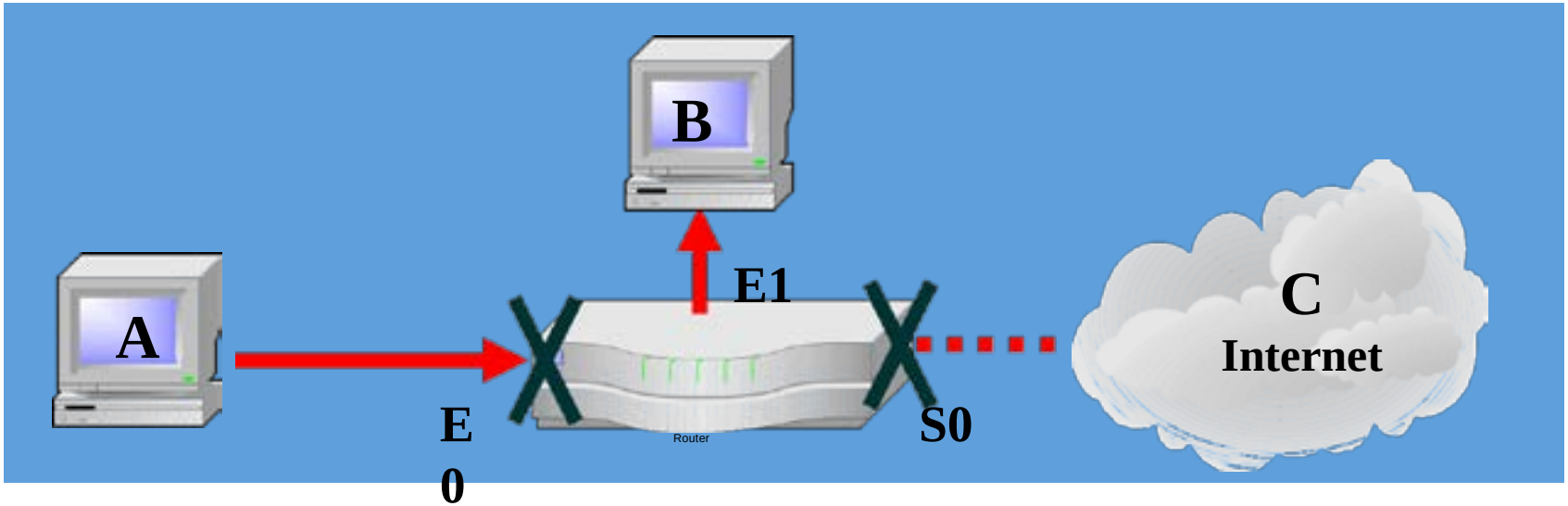
- Par défaut, ce paramètre est configuré sur *out (vers le réseau)*
- Le paramètre *In* (vers le routeur) ou *Out* se place sur l'interface à laquelle on veut appliquer la liste d'accès



Quel port choisir

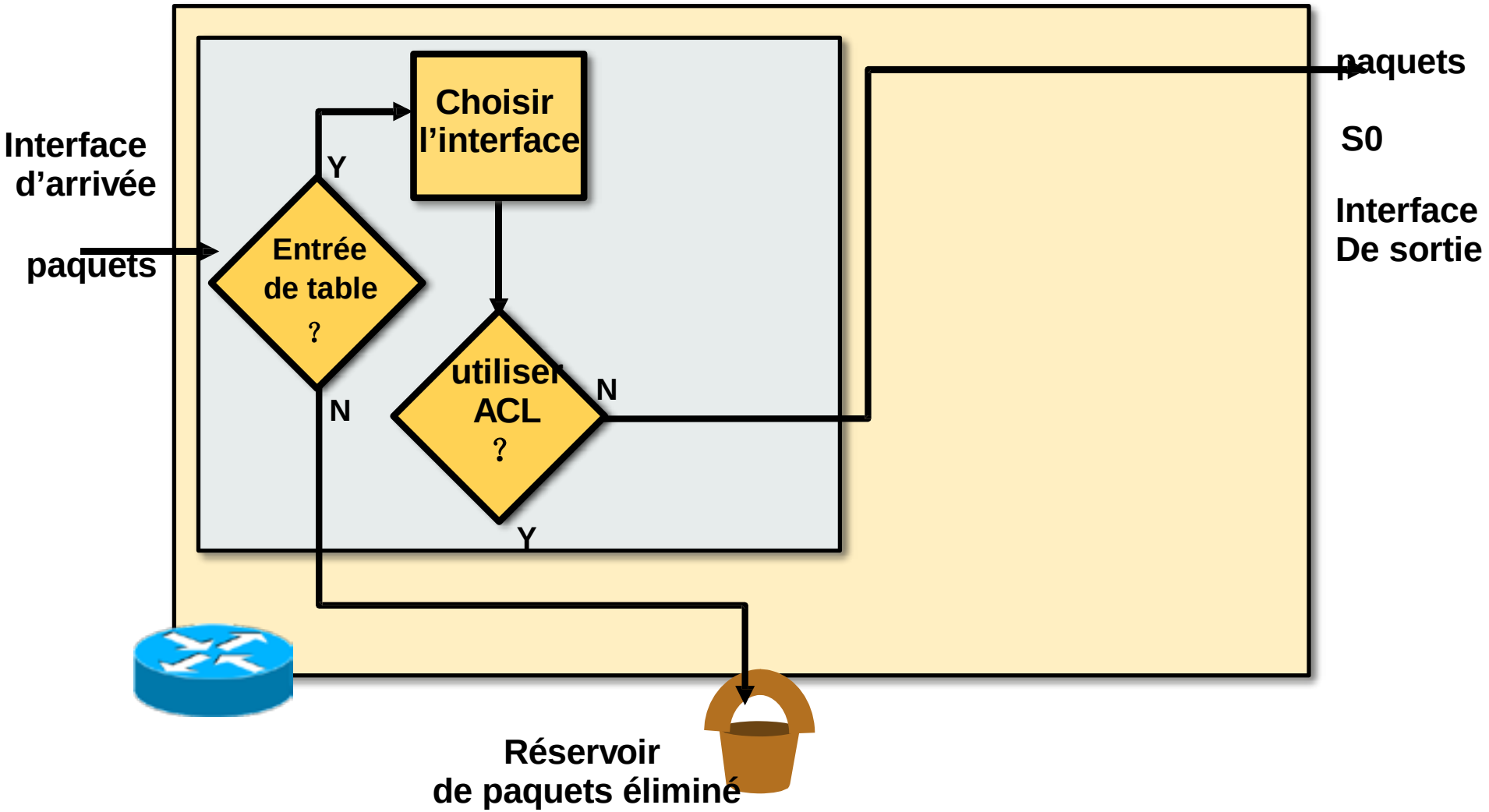
Deux solutions pour bloquer A vers B

- ACL 1 Deny A
- Attribut ACL 1 à l'interface E0 **in**

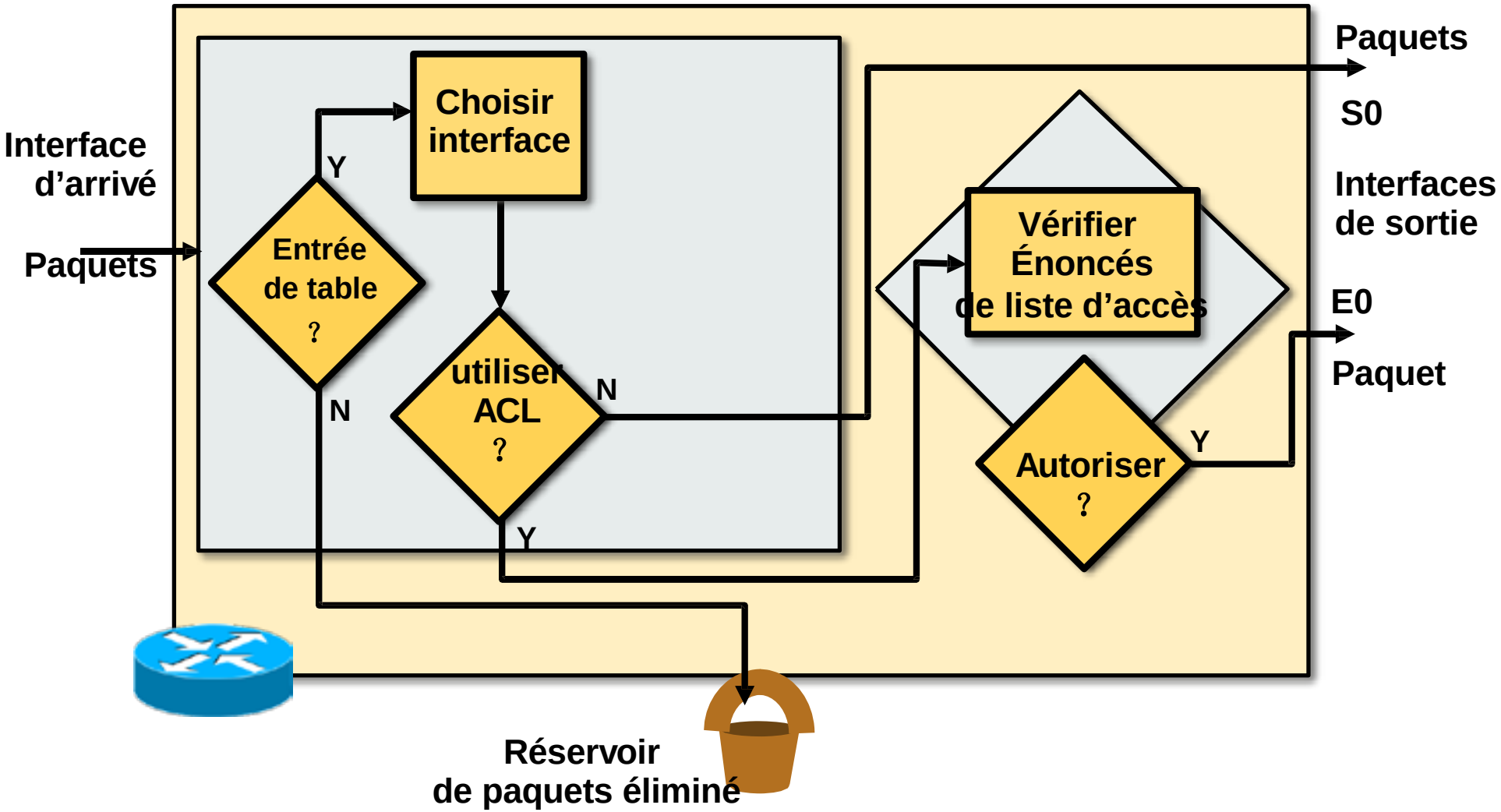


- ACL 1 Deny A
- Attribut ACL 1 à l'interface E1 **out**

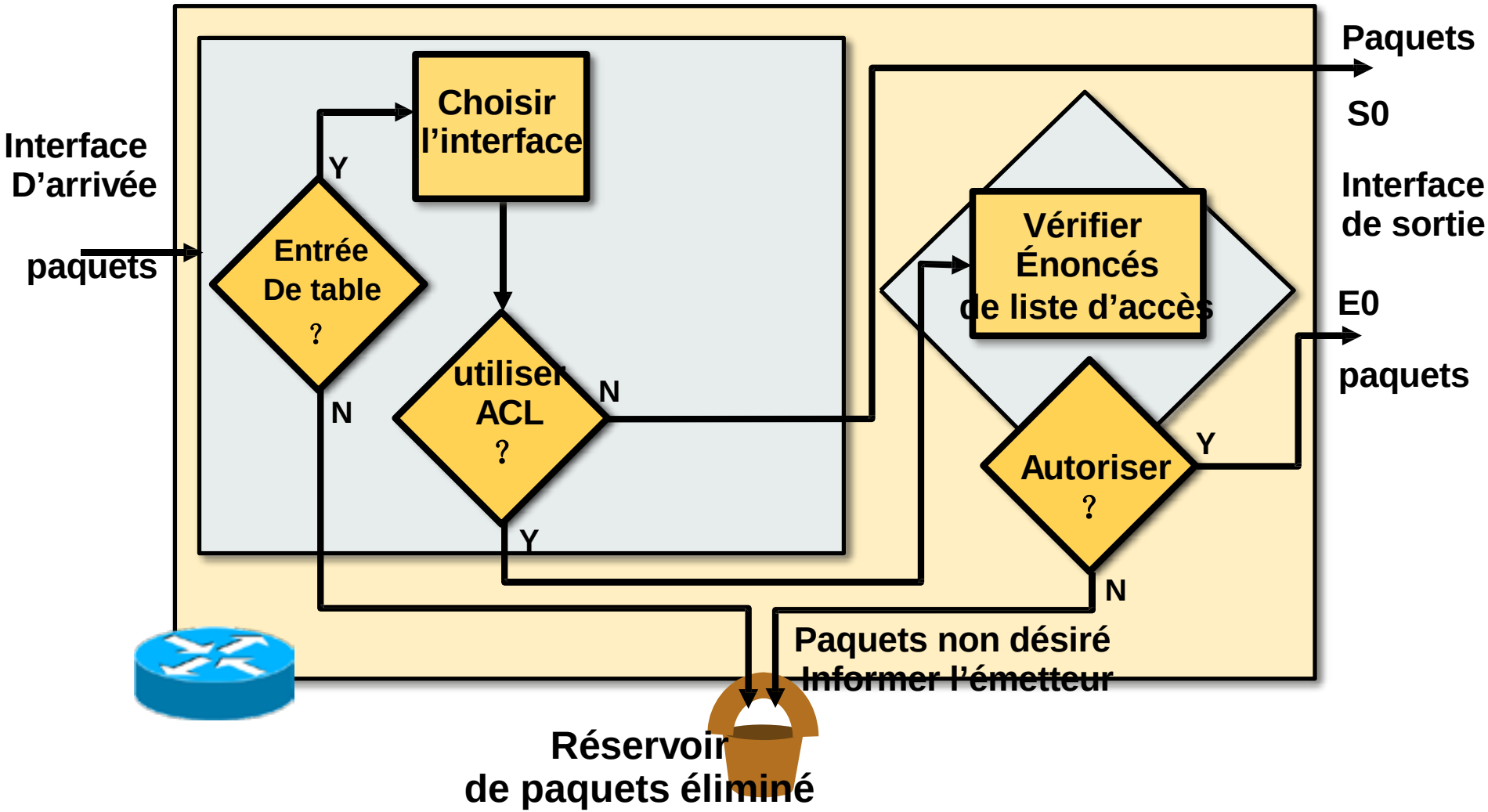
Les processus de contrôle *In* et *Out*(3-1)



Les processus de contrôle *In* et *Out*(3-2)

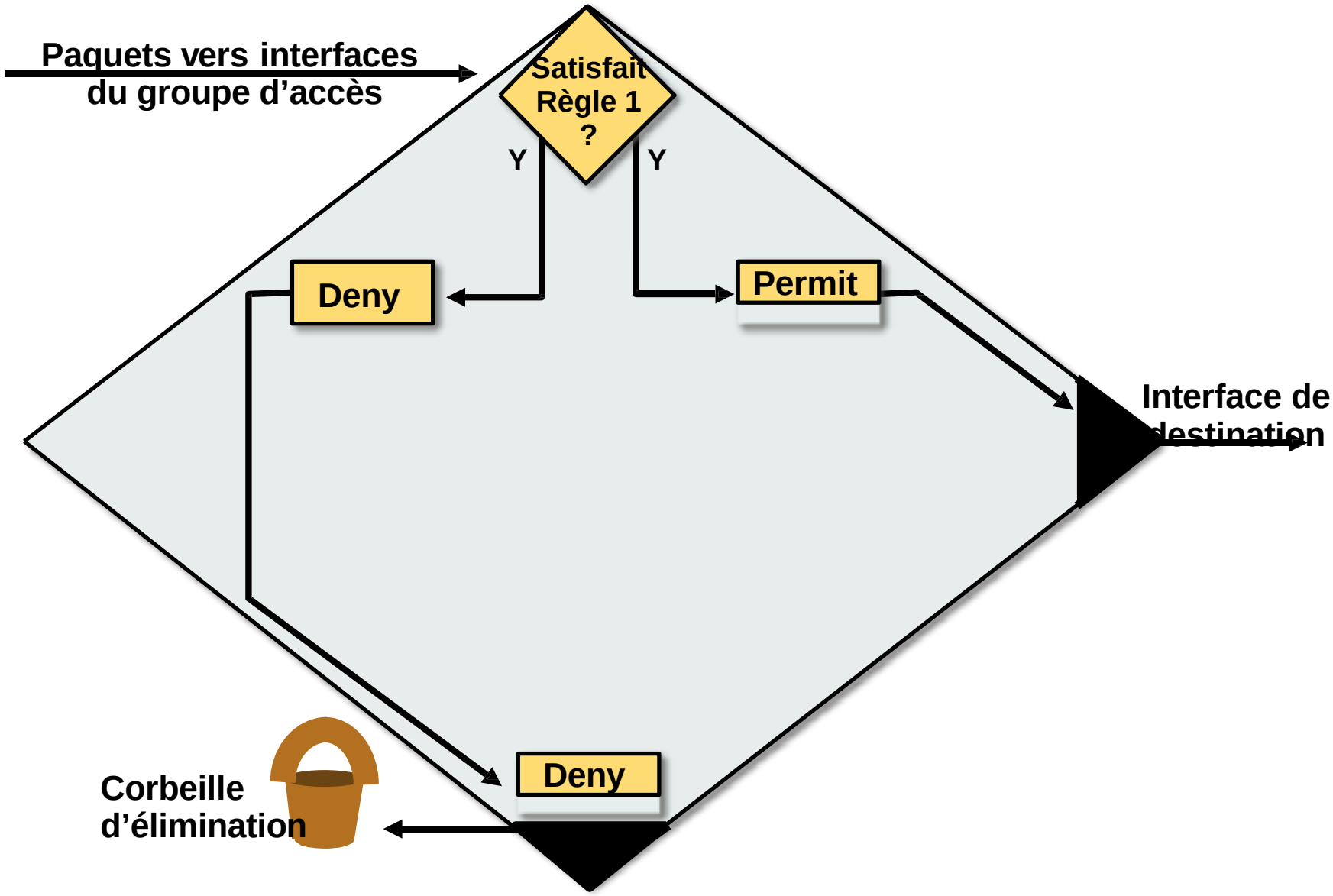


Les processus contrôle de *In* et *Out*(3-3)

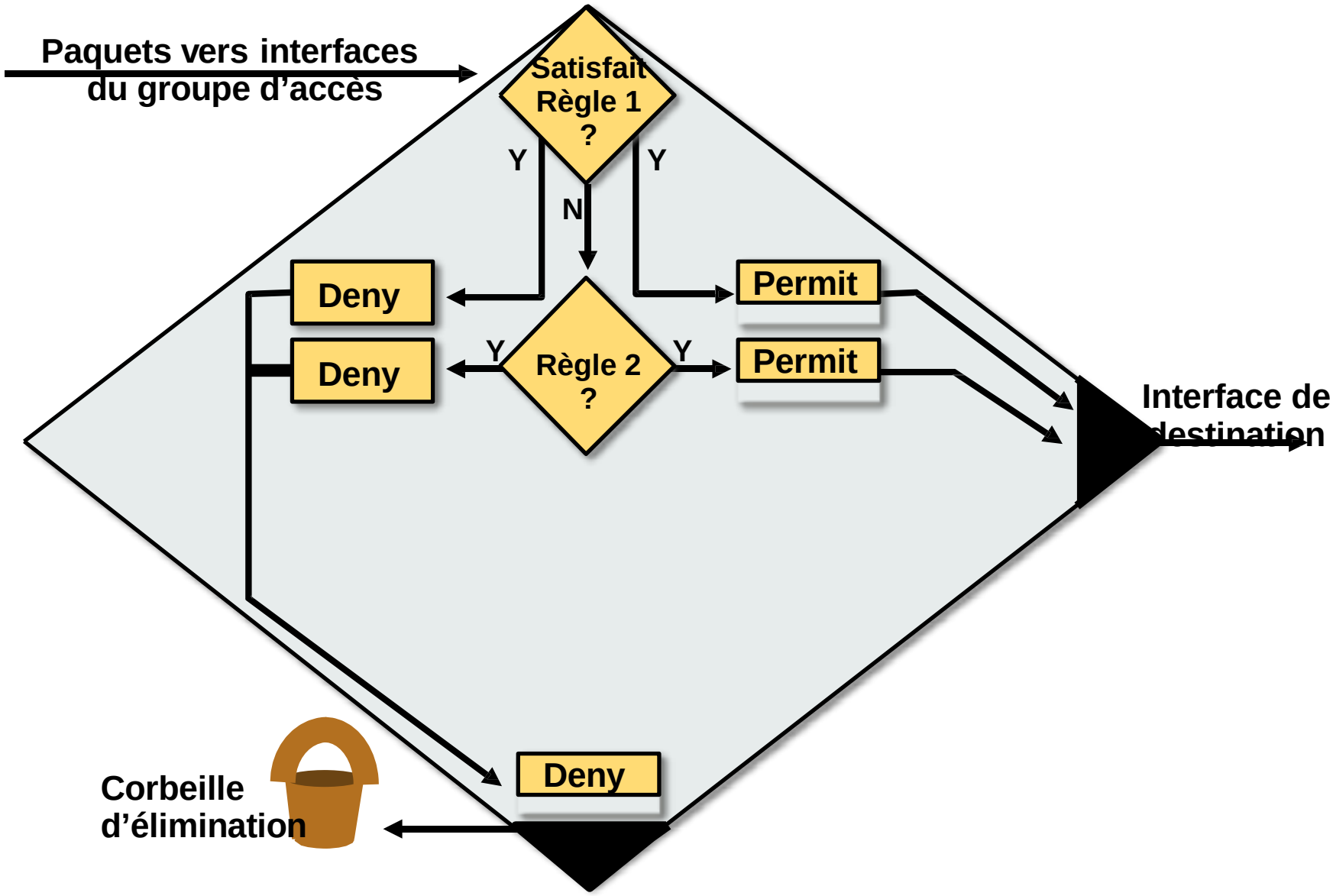


Si il y a aucun matching sur vérifier énoncés de liste d'accès，on rejete le paquet

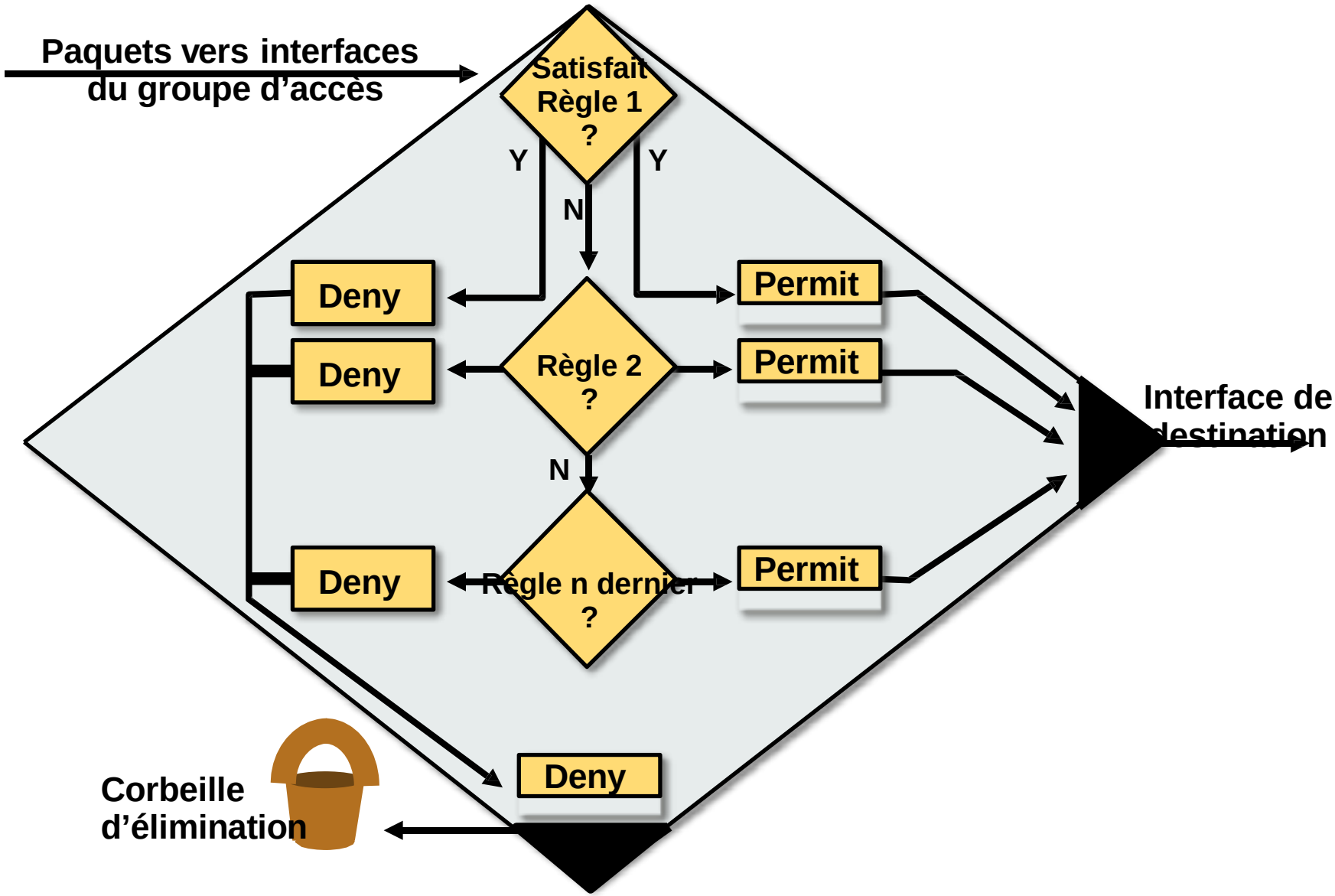
Les processus de vérifier énoncé de ACL(4-1)



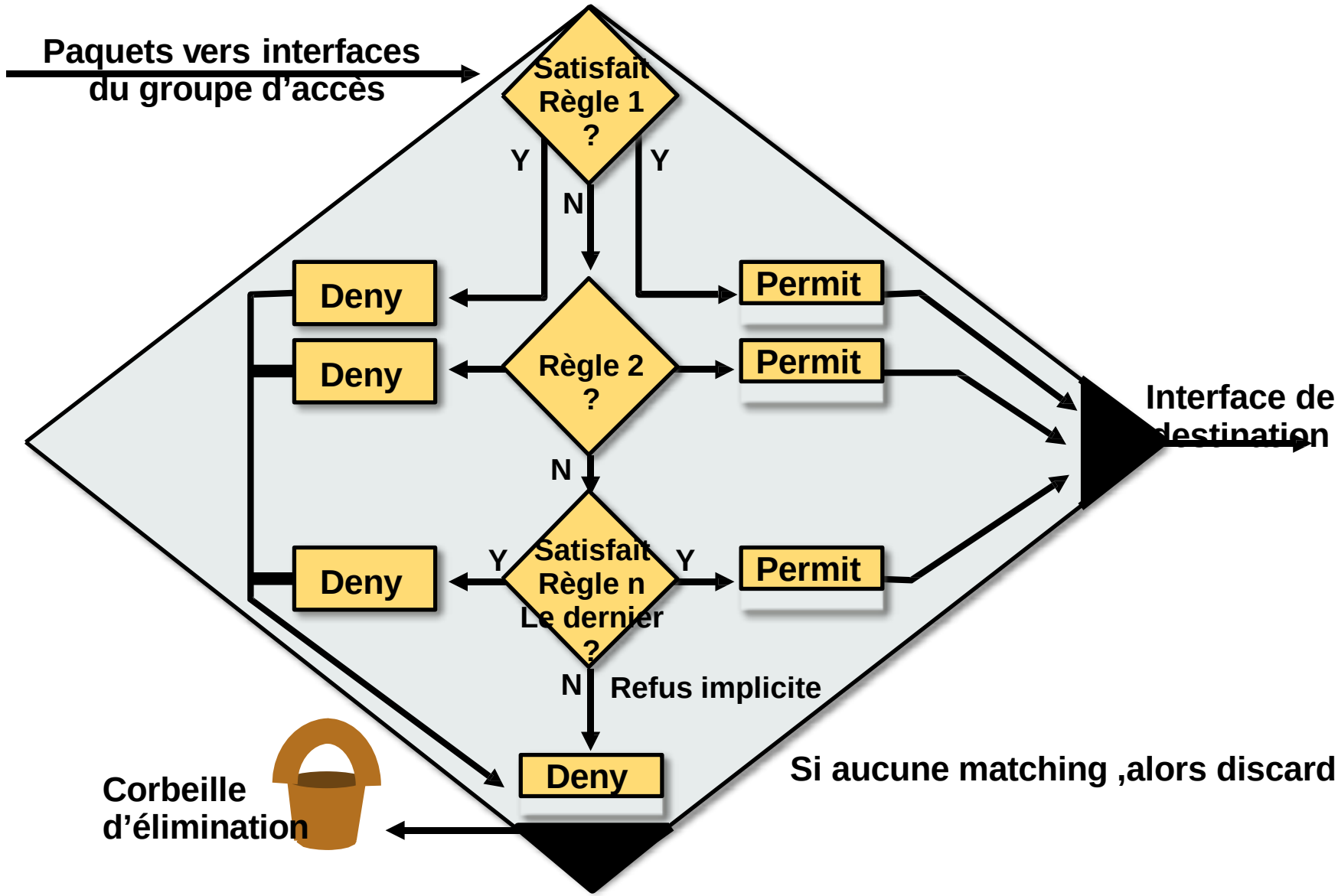
Les processus de vérifier énoncé de ACL(4-2)



Les processus de vérifier énoncé de ACL(4-3)



Les processus de vérifier énoncé de ACL(4-4)



Algorithme de processus

- Algorithme
  - Le routeur teste le paquet par rapport à chaque instruction de condition en partant du début de la liste jusqu'à la fin.
  - Lorsqu'une condition est satisfaite dans la liste, le paquet est accepté ou rejeté et les autres instructions ne sont pas vérifiées.
  - Si une instruction de condition autorisant l'accès à tout le trafic est située en haut de la liste, aucune instruction ajoutée en dessous ne sera vérifiée.
  - Si aucune des instructions ne correspond au paquet, une instruction implicite **`deny any`** est placée à la fin de la liste par défaut.

Commande in et out de ACL

- On utilise ip access-group pour appliquer ACL dans une certaine interface(créer ACL)

```
Router(config)#
 access-list access-list-number { permit | deny } { test conditions }
```

- Une direction de l'interface, on peut utiliser q'une seul access-list(binding ACL à interface)

```
Router(config-if)#
 { protocol } access-group access-list-number {in | out}
```

Commande Deny et permit

Router(config)#access-list *access-list-number* **{permit|deny} {test conditions}**

permet les paquets de passer l'interface qui utilisent ACL

Refuser les paquets

Exemple ACL

- Premier démarche， créer ACL

```
Router(config)#access-list 1 deny   172.16.4.13  0.0.0.0
Router(config)#access-list 1 permit  172.16.0.0  0.0.255.255
Router(config)#access-list 1 permit  0.0.0.0  255.255.255.255
```

- Deuxième démarche ， appliquer la direction out de l’interface e0

```
Router(config)#interface  fastethernet 0/0
Router (config-if) #ip access-group 1  out
```

Références du cours

A. Guermouche, Administration réseau. https://dept-info.labri.fr/~guermouc/