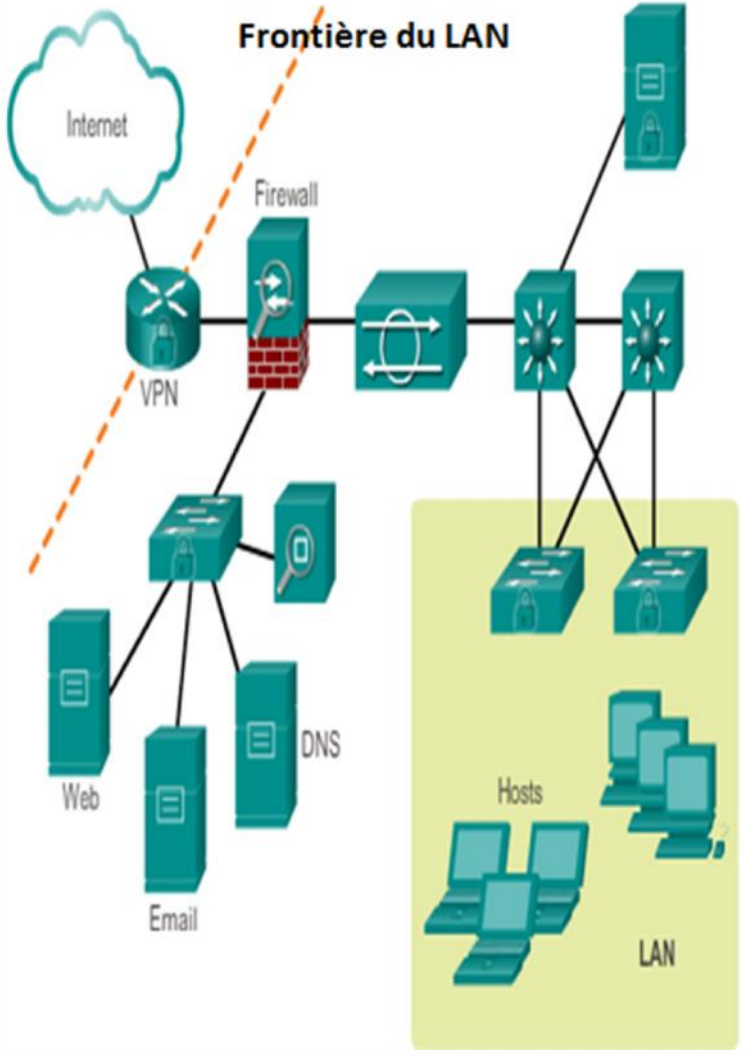
Chapitre 5

LE FILTRAGE DU TRAFIC RÉSEAU

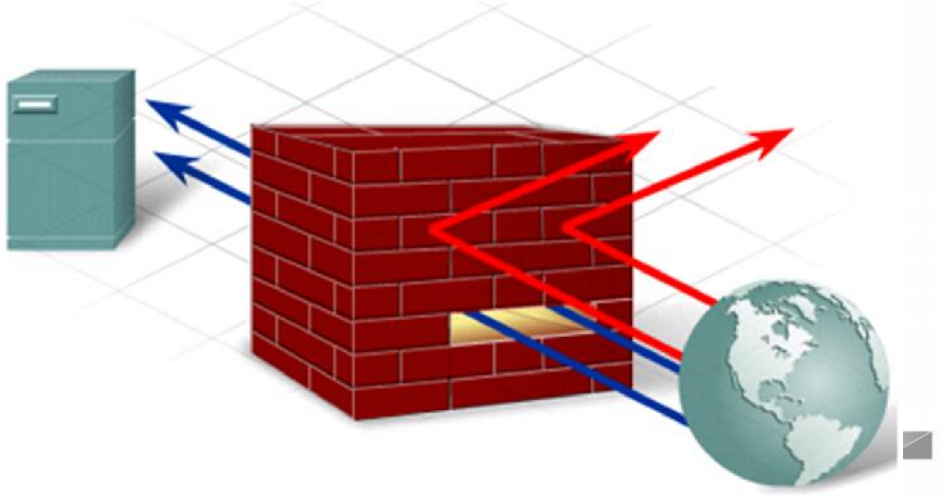
Introduction

- Le réseau Local
  - Un réseau local est une zone privée
  - Le trafic échangé
    - Intérieur ←→Intérieur
    - Intérieur ←→Extérieur
- La protection d'un LAN
  - Que faut il protéger ?
  - Quel type de trafic ?
- Il faut protéger
  - Les nœuds de l'intérieur
  - Les nœuds de bordure

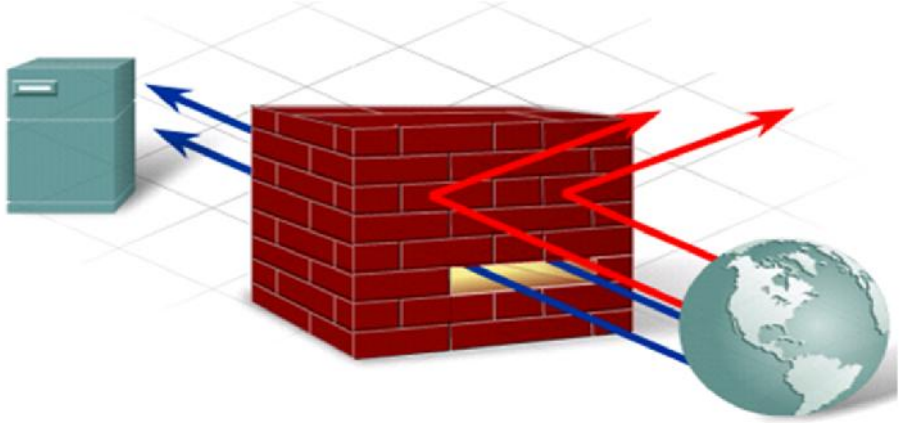


Introduction

- Les nœuds de bordure
  - Constituent la frontière de l'entreprise
  - La portière du trafic externe
- Le trafic externe est
  - non approuvé, n'est pas une source de confiance
  - La source de plusieurs attaques sur le LAN
- La protection contre le trafic externe
  - Réalisée par un **FIREWALL**



Le firewall



- Définition
  - Un firewall, pare-feu, coupe-feu
  - Originalement
    - Il empêche la propagation d'un incendie.
  - Dans un réseau
    - Un firewall doit empêcher la propagation d'une attaque, tout en permettant la circulation du trafic autorisé.
  - Il peut être formé à partir d'un ou plusieurs composants.
- Attention !!
  - Un firewall est inefficace contre les attaques situées du coté intérieur
  - Il ne protège pas contre les attaques qui ne le traverse pas

Le firewall

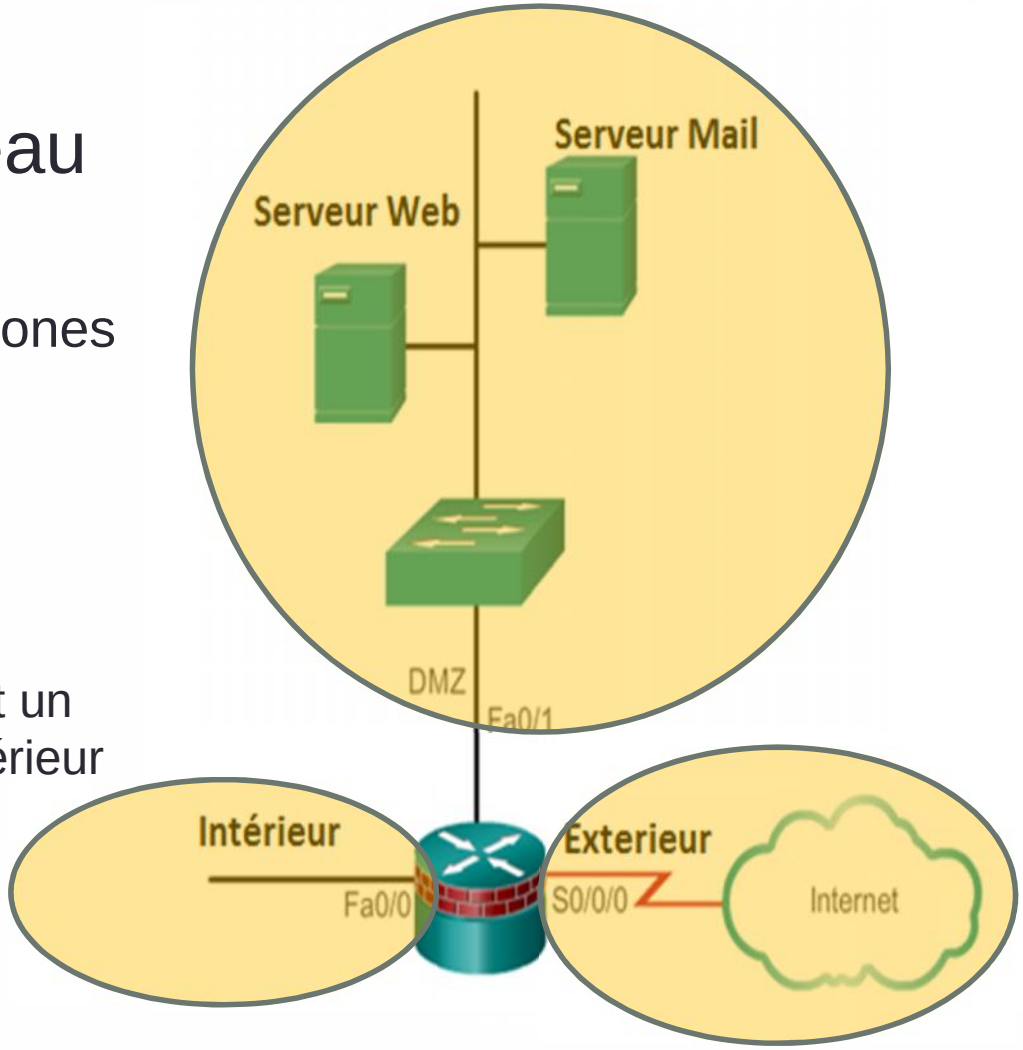
- Définition
  - Un Firewall est un dispositif informatique qui permet **le passage sélectif** des flux d'information entre deux réseaux et qui neutralise les tentatives d'accès qui sont en **désaccord** avec **la politique de sécurité** en appliquée
- Ainsi
  - Sa fonction de base est de réaliser
    - Une inspection sur le trafic transitant
    - Vérifier qu'il est conforme aux règles
    - Laisser passer le « bon » trafic
    - Bloquer, signaler, jetter le « mauvais » trafic
    - **→ Ce qui constitue la fonction de filtrage de trafic réseau**

Le firewall

- Principe de fonctionnement
  - Lit le trafic qui le traverse
  - Analyse le trafic
    - Source
    - Destination
    - Protocole
    - Etat de la connexion
    - Ports utilisés
    - Etc
  - Possède des règles de filtrage
    - Ecrites par l'administrateur
  - Actions à faire
    - **Est-ce que le trafic examiné est conforme aux règles ??**
      - **Oui → laisser passer**
      - **Non → Bloquer**

Le firewall

- Position dans le réseau
  - Typiquement
    - Le firewall sépare trois zones
    - Le LAN (l'intérieur)
    - Le WAN (l'extérieur)
    - La DMZ
      - Zone démilitarisée
      - Zone spéciale autorisant un accès publique de l'extérieur



Le firewall

- Autres fonctionnalités
  - Intelligence artificielle pour détecter le trafic anormal,
  - Filtrage applicatif
    - HTTP (restriction des URL accessibles),
  - Anti Spam
  - Antivirus, Anti-Logiciel malveillant
  - Translation d’adresses (NAT),
  - Tunnels IPsec, PPTP, L2TP,

Le firewall

- Autres fonctionnalités
  - Identification des connexions,
  - Serveur Web pour offrir une interface de configuration agréable.
  - Relai applicatif (proxy),
  - Détection d'intrusion (IDS)
  - Prévention d'intrusion (IPS)
  - Accès de réseau à distance (VPN)
  - Chiffrement
  - Analyse de paquet
  - Journalisation

Le firewall: la base des règles

- L'élaboration des règles de filtrages
  - Action délicate
  - Affecte le fonctionnement d'un firewall
    - Le firewall est inefficace si la règle n'est pas bien écrite
  - Exemple
    - **Première règle: tout autoriser !!!**
    - **`R1(config)# access-list 101 permit ip any any`**
- Les principes de base
  - Moindre privilège
  - Défense en profondeur
  - Goulot d'étranglement
  - Interdiction par défaut
  - Participation de l'utilisateur
  - Simplicité

Le firewall: la base des règles

- Le moindre privilège
  - Ne pas accorder aux utilisateurs du réseau protégé par le pare feu des droits dont il n'ont pas besoin
- Exemple:
  - Interdire le P2P dans une entreprise
  - Interdire FaceBook
  - Interdire les vidéos
  - Limiter la taille du téléchargement
  - Les utilisateurs réguliers ne doivent pas être des administrateurs
  - Les administrateurs doivent également utiliser des comptes utilisateurs

Le firewall: la base des règles

- Défense en profondeur
  - Utiliser les moyens de protection à tous les niveaux possibles
  - Ce qui permet d'évite de laisser entrer des communications indésirables
  - Des moyens autres que le firewall
    - Antivirus
    - Antispam
    - Etc..
- Exemple:
  - Installer des Anti virus à plusieurs niveaux.
    - Sur les PCs, sur les Serveurs, sur un hyperviseur
  - Sécuriser les machines même celles qui sont protégées par le pare feu

Le firewall: la base des règles

- Goulot d'étranglement
  - Toutes les communications entrant ou sortant du réseau doivent transiter par le pare feu.
  - Il ne faut pas avoir plusieurs points d'entrée sur un réseau
- Exemple:
  - Eviter l'utilisation des modems sur le LAN

Le firewall: la base des règles

- Interdiction par défaut
  - En première règle → il faut tout interdire
  - Ensuite autoriser explicitement le trafic « conforme »
  - Ce qui nous permet d'éviter tout transit involontairement accepté
    - Oublier certaines menaces
- Pourquoi?
  - Nous ne pouvons jamais savoir à l'avance toutes les menaces auxquelles nous serons exposer
  - Si nous faisons une erreur
    - **Un trafic « conforme » bloqué mieux qu'un trafic « mal-saint » autorisé!!**

Le firewall: la base des règles

- Participation des utilisateurs
  - Les utilisateur doivent être impliqués dans la mise en place du pare feu.
  - Ils doivent exprimer leurs besoins
  - Ils recevront en échange les raisons et les objectifs de la politique de sécurité
- Les contraintes du pare feu seront acceptées
  - Moins d'objections
  - Comprendre les besoins de l'utilisateur
  - S'assurer que les raisons de restrictions sont bien comprises

Le firewall: la base des règles

- La simplicité d'une règle
  - Les règles de filtrage du pare feu doivent être les plus simples
  - Pour assurer qu'elles compréhensibles
  - Eviter toutes les erreurs de conception
  - Il serait plus facile de vérifier le bon fonctionnement

Les types de firewall

- Un firewall peut être
  - Un boîtier dédié
    - C'est un matériel
    - Noté « appliance »
  - Un logiciel
    - Peut être un système d'exploitation
    - ou un logiciel dédié
  - Les bastions (Serveurs mandataires)
    - Proxy, relais applicatif
  - Un routeur
    - Configurer avec des ACLs,

Les types de firewall

- Un firewall peut être
  - Firewall Logiciel
  - Un poste de travail standard avec un logiciel pare-feu
  - Exemple: (IP Cop, IPTables,…etc)
- Firewall matériel
  - Une boîte noire spécial
    - qui contient aussi un logiciel
  - Exemple:
    - CISCO PIX, Juniper, FortiGate, StoneGate

Les types de firewall

- Un firewall matériel ou logiciel ??
  - Un pare-feu logiciel hérite toutes les vulnérabilités du système d'exploitation sur lequel ils s'exécute
  - L' architectures du pare-feu logiciel est connu, donc c'est plus facile à exploiter ses vulnérabilités
    - exemple : buffer overflow

Les types de firewall

- Le proxy firewall
  - Relai entre deux entités
  - Analyse le contenu des données de l'application
  - Dédié à une application
    - proxy http
    - proxy ftp
    - Etc,
- Principe
  - Il faut spécifier au niveau de l'application l'existence du proxy
  - Complètement transparent à l'utilisateur

Les types de firewall

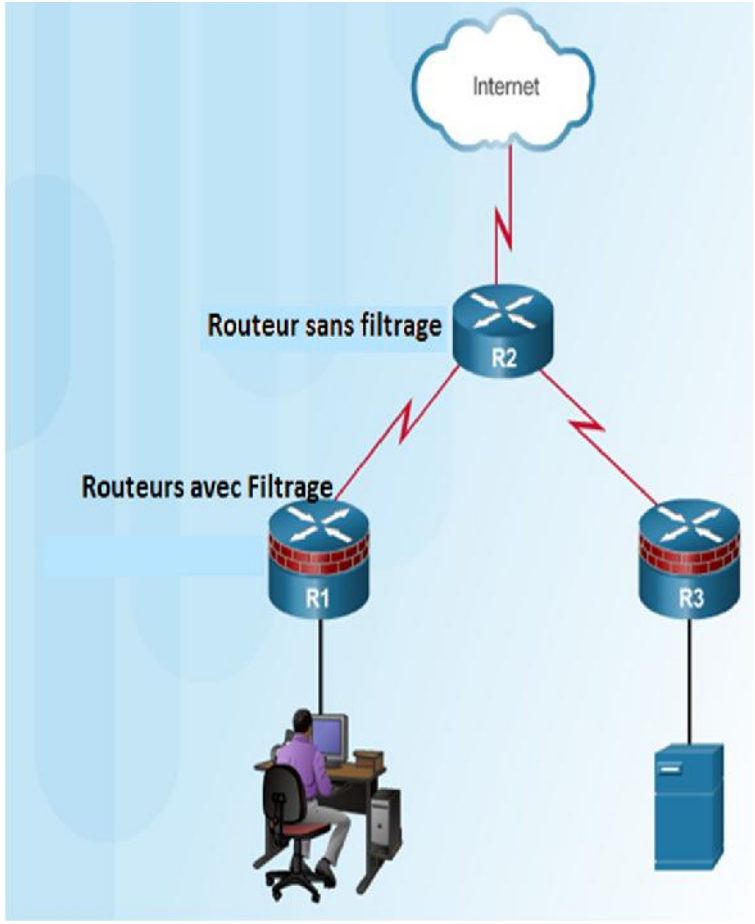
- Le proxy firewall
  - Permet de faire du cache
  - Permet d'effectuer certains filtres
    - Suivant les comptes utilisateurs pour FTP par exemple
    - Suivant les adresses sources...
    - Contenu des pages WEB ...
    - Détection de virus
  - Permet de faire des statistiques

Le firewall: niveau de fonctionnement

- Sur quelle couche du modèle OSI?
  - Le firewall peut fonctionner sur différents niveau
  - Filtrage au niveau paquet
    - Niveau 3 du modèle OSI
      - Filtrage par : IP source ou destination
      - Filtrage par : Protocoles (TCP, UDP, ICMP,…etc)
  - Filtrage par état de connexion
    - Niveau 4 du modèle OSI
      - Filtrage par : Flags et options (ACK, SYN,…etc)
  - Filtrage Applicatif
    - proxy HTTP, FTP, SMTP,…etc)
  - Translation d'adresse
    - Réalise du NAT
    - Cacher l'architecture privée du LAN

Le firewall: niveau de fonctionnement

- Le filtrage paquet
  - Généralement une partie d'u routeur
  - Possédants des « listes de contrôle d'accès » ACL
  - Examine l'entête d'un paquet
- Fonctionnement simple
  - Table de politiques
    - Autorisant ou bloquant un trafic selon des critères
      - Adresse IP, source et destination
      - Protocoles
      - Ports source et destination
      - Etat de connexion TCP

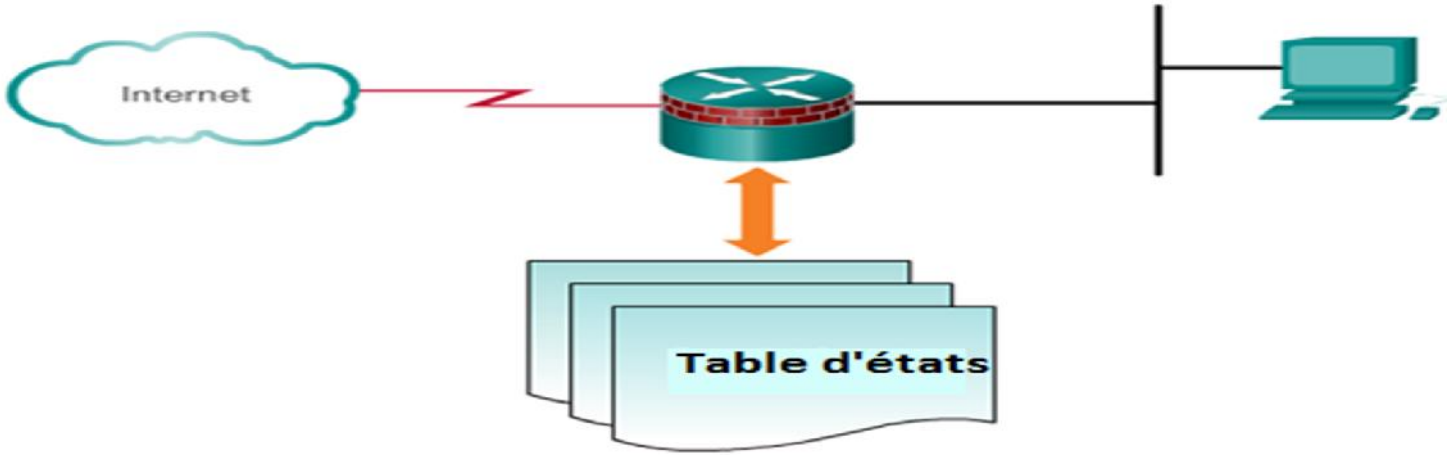


Le firewall: nature du filtrage

- Avec ou sans mémoire
  - Est-ce que le firewall reconnait un trafic déjà examiné
- Deux modes
  - Firewall sans mémoire
    - Ne se souvient pas des paquets qu'il a déjà vu
  - Firewall avec mémoire
    - Garde une trace des paquets qui passent par lui.
    - Reconstruit l'état de chaque connexion

Le firewall: niveau de fonctionnement

- Le filtrage avec mémoire
  - Les plus répandus et les plus utilisés
  - Appelé aussi « **filtrage paquet avec état** »
  - Examine la couche 3 et la couche 4
  - Le firewall
    - Maintient une table d'état de connexion
    - Il enregistre toutes les communications dans cette table
    - Reconnait les applications et les connexions dynamiques qu'elles vont ouvrir



Le firewall

- Exemple de règles

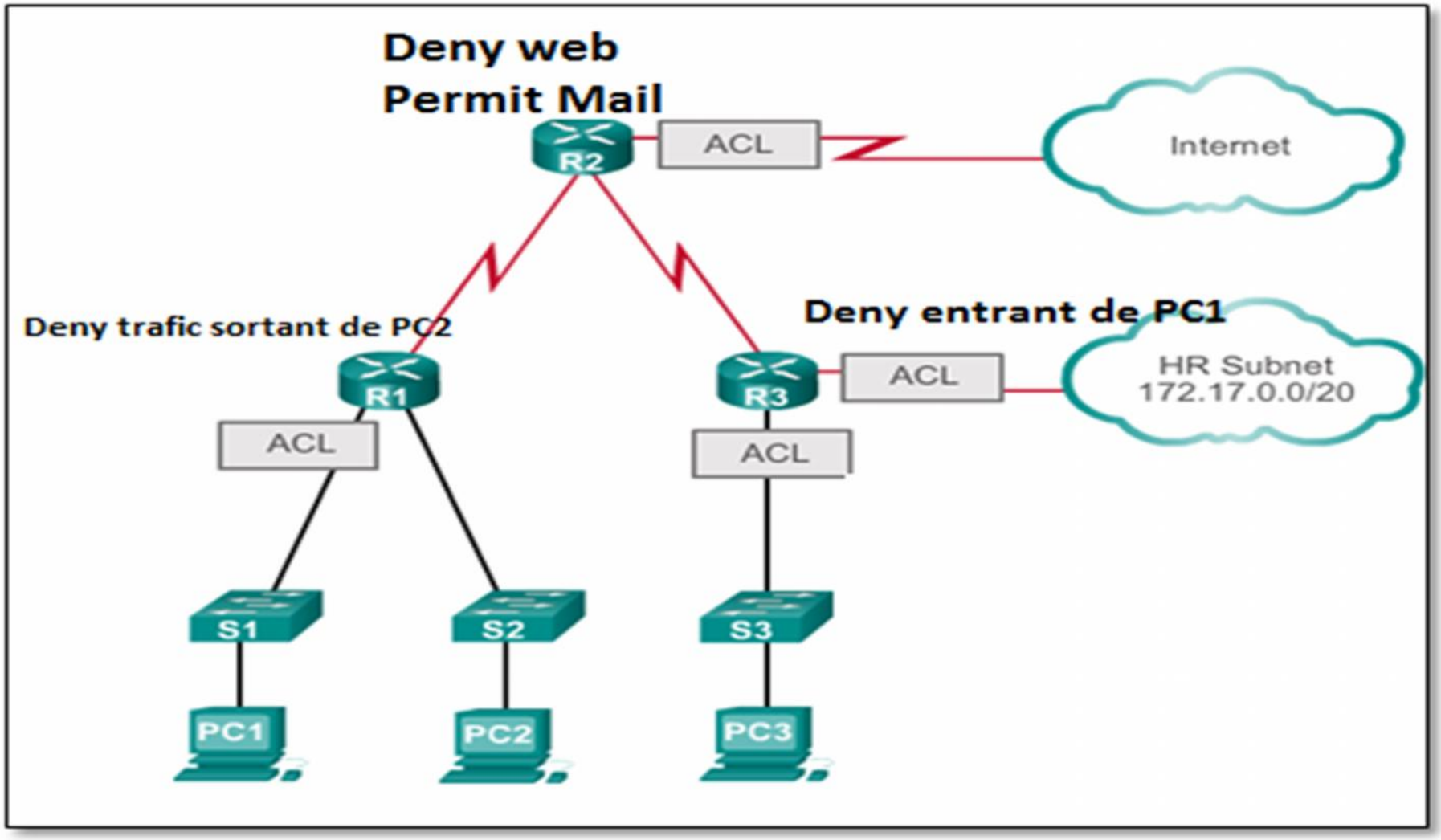
	src	port	dst	port	protocol	action
1	any	any	128.12.1.2	25	TCP	permit
2	128.12.1.2	25	any	any	TCP	permit
3	128.12.1.2	any	any	25	TCP	permit
4	any	25	128.12.1.2	any	TCP	permit
5	any	any	any	any	TCP	deny

ACCESS CONTROL LISTE

Les listes de contrôle d'accès

- Présentation
  - Technique de filtrage largement utilisée dans les réseaux d'entreprise
  - Généralement implémentées au niveau des routeurs
- Principe
  - Liste de trafic (accepté ou refusé) configurée et activée au niveau des équipements de bordure
- Avantages
  - Simple
    - Action claire (permit /deny), par couche
  - Efficace
    - Par port, service, protocole, adresse, plage d'adresses, état, temps, etc..
  - Faible coût

Les listes de contrôle d'accès



Les listes de contrôle d'accès

- Présentation
  - Une ACL est identifiée par son numéro ou un nom
    - Variant de 1 →2699
  - Grace au numéro on classe les ACLs en deux catégories
    - Standard
    - Etendue
- Exemple
  - ACL IP Standard
    - Numéro 1→99 et 1300 →1999
  - ACL IP Etendue
    - Numéro 100→199 et 2000→2699

ACL standard

- Numéro
  - Numéro 1→99 & 1300→1999
- Rôle
  - Ne peut examiner que l'adresse IP source de l'entête de chaque paquet IP
- Usage
  - Filtrage global par adresse IP
  - Filtrage léger
  - Pas de surcharge sur le routeur
- Application
  - Sur les interfaces (entrée et/ou sortie)
  - Par groupement IP

ACL étendue

- Numéro
  - Numéro 100→1299 & 2000→2699
- Rôle
  - Peut filtrer les paquets IP en se basant sur
    - Adresse IP: source et destination
    - Type de protocole
    - Numéro de port source et destination
- Usage
  - Filtrage plus efficace que les ACLs standards
  - Action plus orientée et plus spécifique
- Application
  - Sur les interfaces (entrée et/ou sortie)
  - Par groupement IP

Liste complète des numéro ACLs

Protocole	Plage
IP	1-99, 1300-1999
Extended IP	100-199, 2000-2699
Ethernet type code	200-299
DECnet and Extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
AppleTalk	600-699
Ethernet address	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Extended transparent bridging	1100-1199

ACL standard et Etendue

- Exemples :ACL nommées
  - Ligne de commande
- `Router(config)# ip access-list [standard | extended] name_of_ACL`
- Standard

```
R1(config)# ip access-list standard NO_ACCESS
R1(config-std-nacl)# deny host 192.168.11.10
R1(config-std-nacl)# permit any
R1(config-std-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group NO_ACCESS out
```

ACL standard et Etendue

- Exemples :ACL nommées
  - Ligne de commande
- `Router(config)# ip access-list [standard | extended] name_of_ACL`
- Etendue

```
R1(config)# ip access-list extended SURFING
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 80
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq 443
R1(config-ext-nacl)# exit
R1(config)# ip access-list extended BROWSING
R1(config-ext-nacl)# permit tcp any 192.168.10.0 0.0.0.255 established
R1(config-ext-nacl)# exit
R1(config)# interface g0/0
R1(config-if)# ip access-group SURFING in
R1(config-if)# ip access-group BROWSING out
```

Configuration d'une ACL

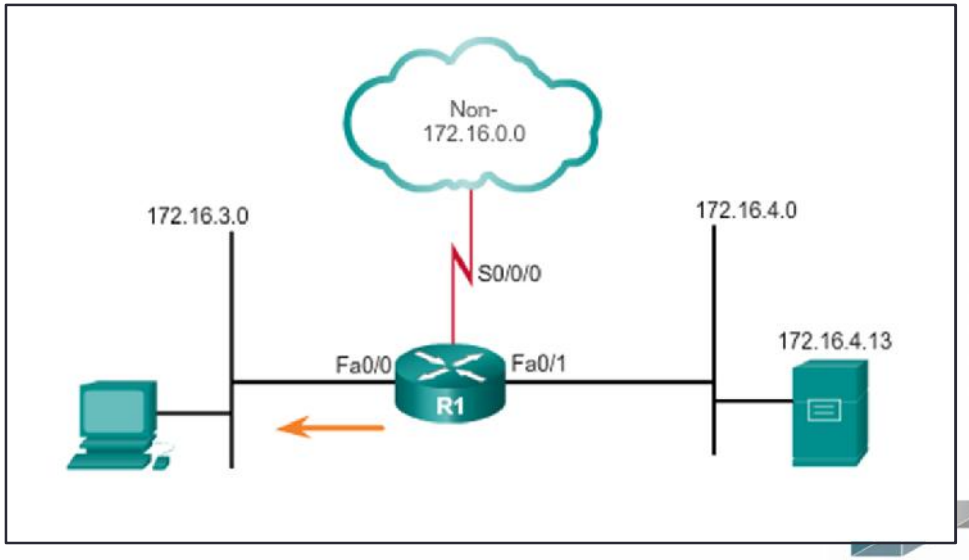
- ACE: Access Control Entry
  - Une ACL peut être construite par une ou plusieurs **entrées**
  - Une entrée représente une règle indépendante
- Les règles d'écritures des ACEs
  - **Interdiction implicite** « **Implicit deny all** »
  - **Ordre d'écriture**
    - Les ACLs sont traitées selon le principe « premier correspondant »
      - Après la première correspondance **Le reste de la liste** n'est plus examiné
    - Attention
      - Ne pas commencer par une négation totale
      - Commencer par le plus spécifique vers le plus général

Configuration d'une ACL

- Les règles d'écritures des ACEs
  - **Filtrage directionnel**
    - Une ACL peut être appliquée en entrée (**Inbound**) ou en sortie (**Outbound**)
  - **Paquet spécial**
    - Les ACLs ne s'appliquent pas sur les paquets spéciaux
      - Les paquets de routage
      - **En réalité n'est pas toujours respectée !!**
  - **Modification des ACLs**
    - Chaque nouvelle entrée est ajoutée à la fin
      - Ce qui affecte le fonctionnement!!!
    - Idée: Numéro de séquence de ACE
      - Optionnel
      - Il permet de donner un numéro à chaque entrée

Configuration d'une ACL

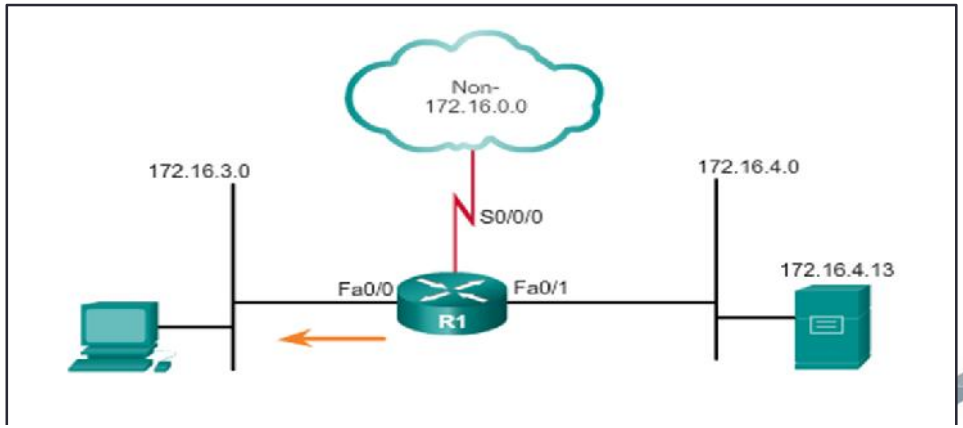
- Exemple ACL standard
  - Action:
    - **bloquer le trafic allant du sous réseau R1 vers R2 et autoriser tout le reste**
- `R1(config)# access-list 1 deny 172.16.4.0 0.0.0.255`
- `R1(config)# access-list 1 permit any`
- `R1(config)# interface FastEthernet 0/0`
- `R1(config-if)# ip access-group 1 out`



Configuration d'une ACL

- Exemple ACL étendue
  - Action:
    - **bloquer le trafic FTP allant du sous réseau R1 vers R2 et autoriser tout le reste**

```
R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21
R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20
R1(config)# access-list 101 permit ip any any
R1(config)# interface FastEthernet 0/0
R1(config-if)# ip access-group 101 out
```



Modification d'une ACL existante

```
Router# show access-lists
Extended IP access list 101
    10 permit tcp any any
    20 permit udp any any
    30 permit icmp any any
```

Modifier ACE 20

Ajouter ACE 05

```
Router(config)# ip access-list extended 101
Router(config-ext-nacl)# no 20
Router(config-ext-nacl)# 5 deny tcp any any eq telnet
Router(config-ext-nacl)# 20 deny udp any any
```

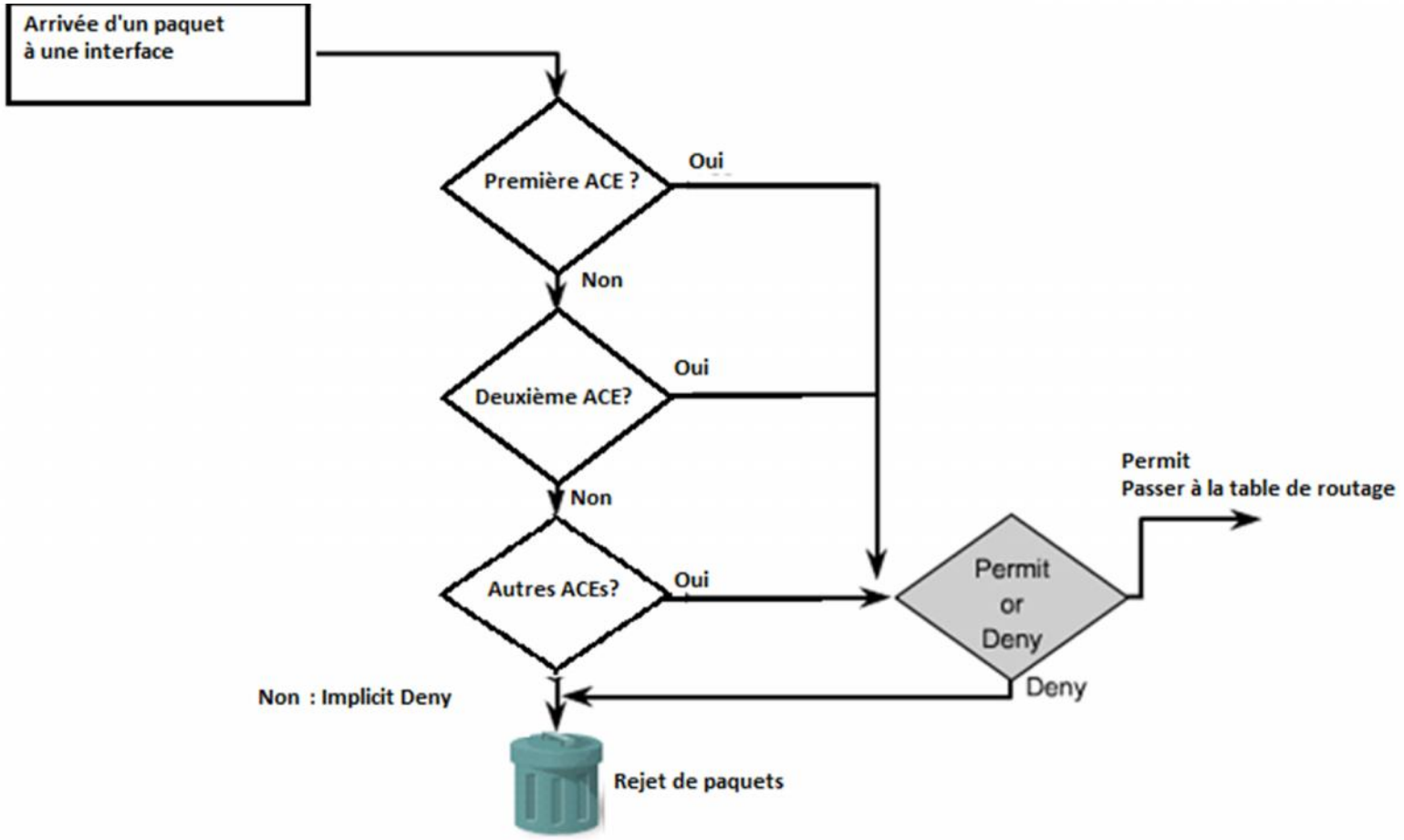
```
Router# show access-lists
Extended IP access list 101
     5 deny tcp any any eq telnet
    10 permit tcp any any
    20 deny udp any any
    30 permit icmp any any
```

Application des ACLs

- Définition technique « la vision du Routeur »
  - Quelle est la direction du trafic????
- Inbound ou entrant
  - Un trafic est dit « Inbound » à une interface lorsque ce trafic traverse cette interface **avant** qu'il soit traité par la table de routage
- Outbound ou sortant
  - Un trafic est dit « Outbound » à une interface lorsque ce trafic traverse cette interface **après** avoir été traité par la table de routage

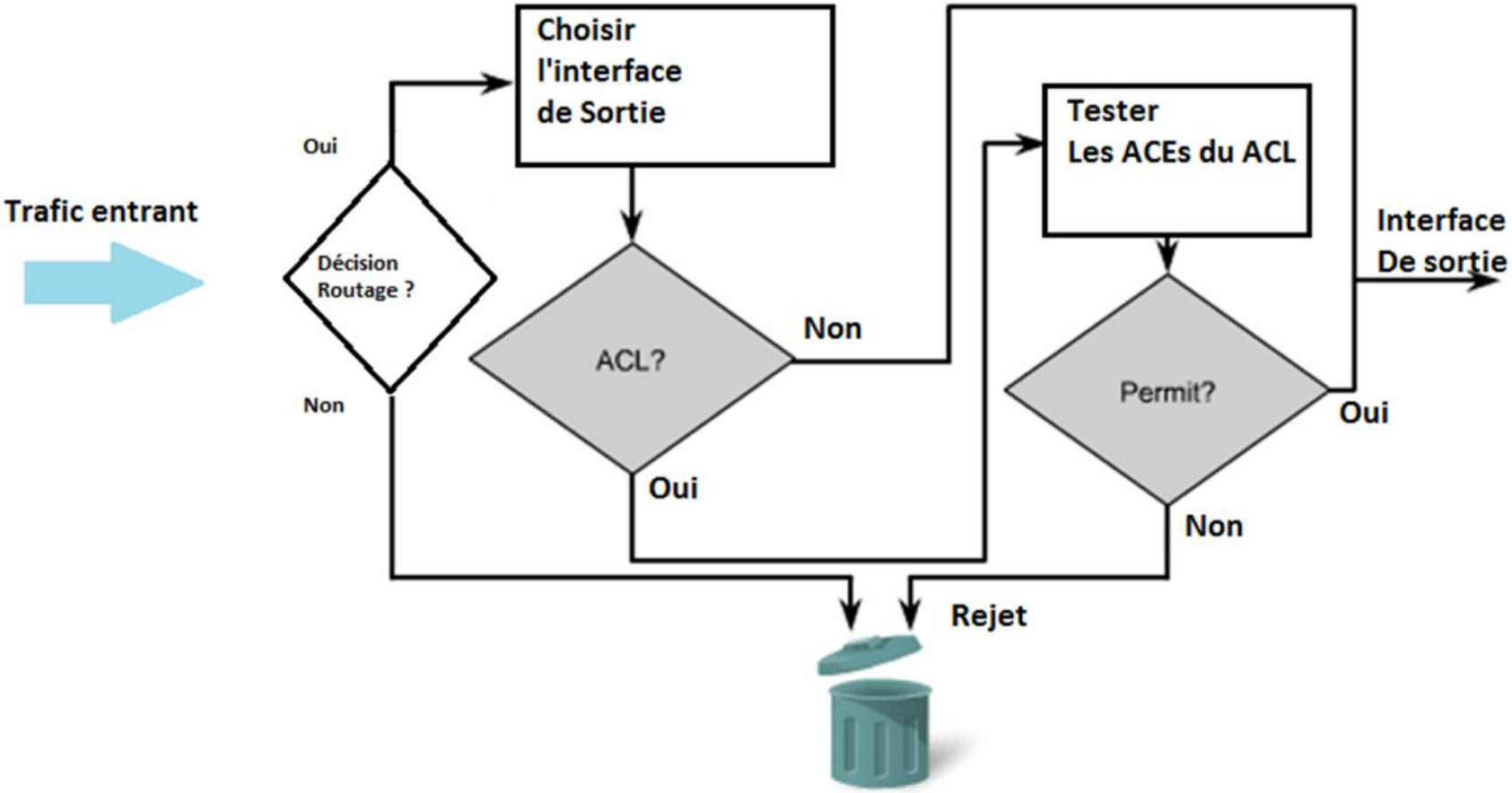
Application des ACLs

- Organigramme d'application: Inbound



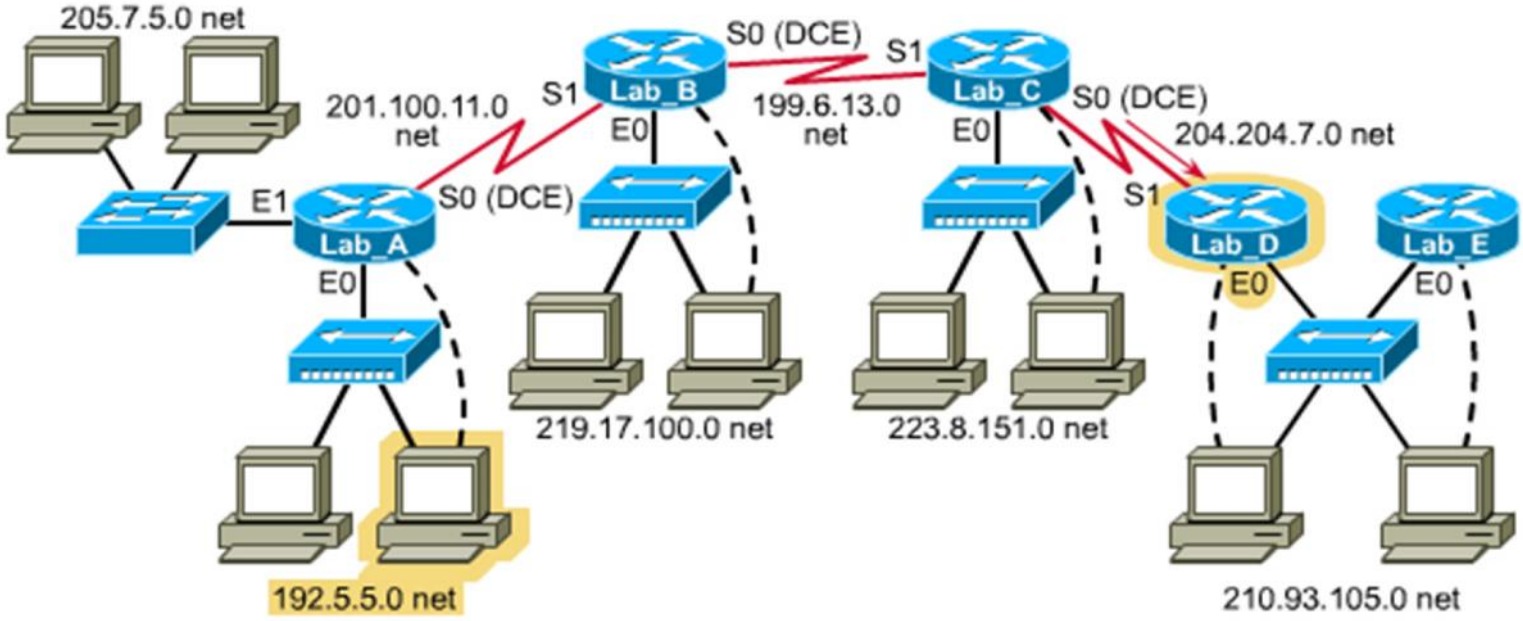
Application des ACLs

- Organigramme d'application: Outbound



Choix de l'emplacement d'une ACL

- Les Acls standards
  - Aucune indication sur la destination
  - Donc → il faut les placer le plus **proche** possible de la destination
- Exemple: objectif interdire 192.5.5.0 sur LAB-D
  - **Quel emplacement (Lab-A E0-entrant ou LAB-D-E0-sortant)**



Choix de l'emplacement d'une ACL

- Les Acls étendues
  - Porte une indication sur la destination
  - Donc → il faut les placer le plus proche possible de la source
- Placer les ACLs étendues loin de la source
  - peut être inefficace
  - gaspillage de ressources et mauvaise exploitation
  - **→un Trafic qui sera finalement bloqué pourquoi l'amener plus loin!!**

Autres types d'ACLs

- Option « established »
  - Créée en 1995
  - Permet de traquer l'état de connexion TCP
  - Bloque tout le trafic TCP qui n'est pas initialisé de l'intérieur de la société
  - Vérifie l'état du flag (ACK/RESET)
    - Si ACK n'est pas activé→ trafic refusé
  - Considérée comme la première génération de Firweall avec état

```
R1(config)# access-list 100 permit tcp any eq 443 192.168.1.0 0.0.0.255 established
R1(config)# access-list 100 deny ip any any
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 100 in
```

Autres types d'ACLs

- Par intervalle de temps
  - ACL appliquée par tranche de temps

```
R1(config)# time-range EVERYOTHERDAY
R1(config-time-range)# periodic Monday Wednesday Friday 8:00 to
17:00
```

```
R1(config)# interface s0/0/0
R1(config-if)# ip access-group 101 out
```

Autres types d'ACLs

- Reflexive ACL
  - Plus complexe créée en 1996
  - Capable d'identifier les sessions d'un trafic
    - Filtrage en même temps par: Source, destination et port
  - Utilisation
  - Permet d'autoriser les sessions (intérieur vers l'extérieur) et bloquer l'autre sens
- ACL Dynamique
  - ACL qui s'applique dynamiquement
  - Combinée avec telnet
  - Permet d'authentifier les utilisateurs
    - Ils seront bloqués jusqu'à ce qu'ils accèdent par telnet
    - Ensuite ils seront acceptés
    - Si leur sessions est fermée→ bloquer de nouveau