Le mécanisme de filtrage (IP)

# I. Introduction

Faire du filtrage sur IP, sur l’entête IP : ACL (Access Control List). Filtrer suivant des critères sur l’entête IP.

Au niveau des paquet IP : filtrage sur les paquets entrant/sortant suivant (@IPsource, @IPdestination).

Protocole pour envoyer les mails : SMTP (25), iMAP (143), POP (110)

|  |  |
| --- | --- |
| N° port : TCP/UDP | Bloc de données |

|  |  |
| --- | --- |
| IP : Entête | Bloc de données |

2 types d’ACL :

* **ACL standard (**filtrage uniquement sur IP)
* **ACL étendu** (analyse de la partie correspondant à la partie TCP/UDP)

# II. Fonctionnement

Routage

Accept

Traffic entrant

Deny

Trash

Deny

Accept

Traffic sortant

Le paquet est vérifié par rapport au 1er critère :

* Le paquet passe aux ACLs suivants
* Si un critère n’est pas satisfait, le paquet est rejeté.

Élément actif pour le filtrage : routeur (Cisco est le leader).