Université de M’sila
Département d’informatique
Master2 Réseaux

LISTE DE CONTRÔLE D’ACCÈS

Saoudi Lalia

2019-2020

Présentation

- Une ACL est une liste de règles
  - permettant d'interdire ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, ...
  - Elles opèrent selon un ordre séquentiel et logique.
  - Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output).

Création des ACL – Généralités

- Pour créer une liste de contrôle d’accès, il faut :
  - Créer la liste de contrôle d'accès en mode de configuration globale.
  - Assigner cette ACL à une interface

a)Structure générique d’une ACL :

- Router(config)#access-list *numéro d’ACL* {permit|deny} *instructions*

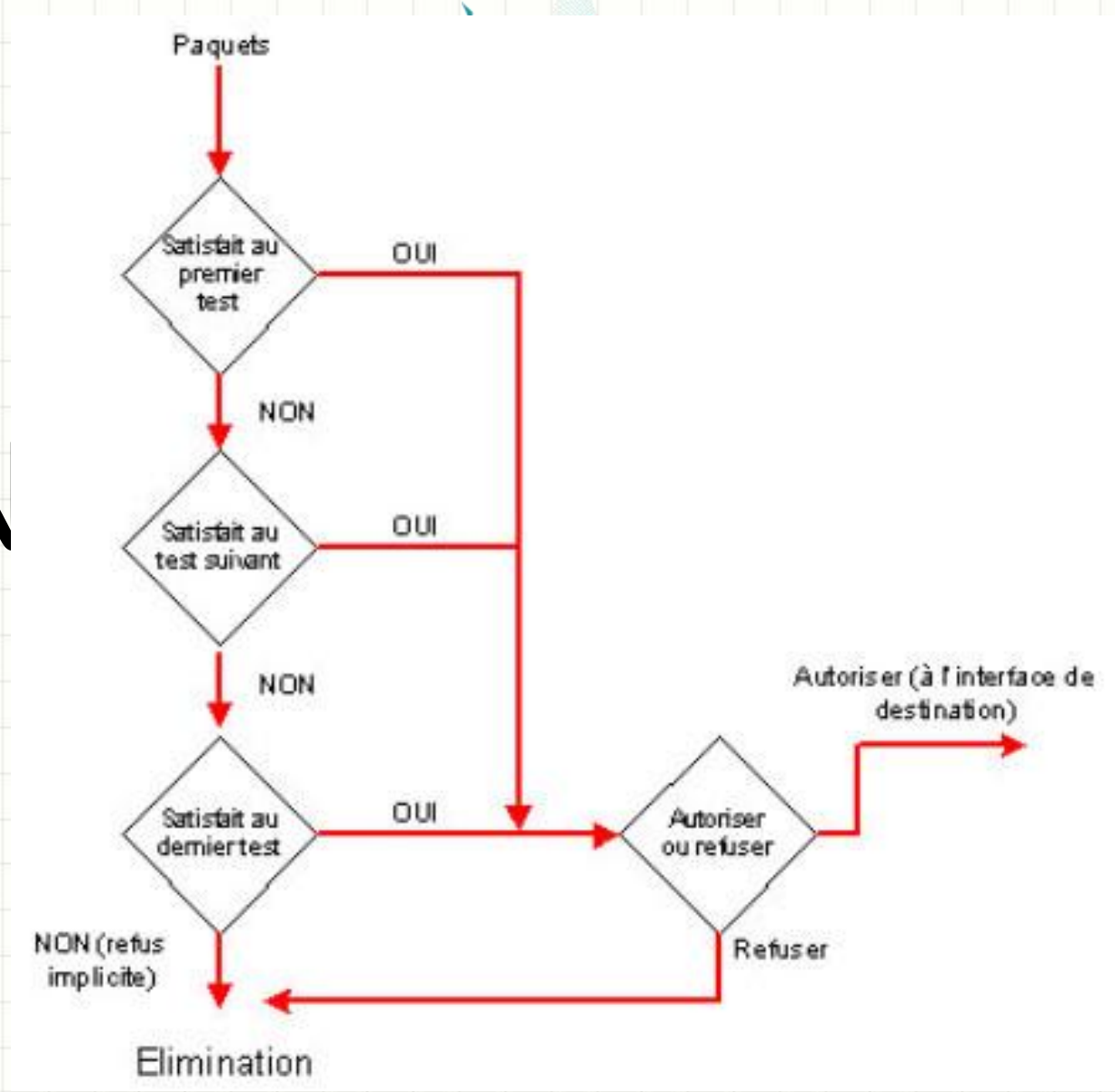
Concevoir une ACL

- Lorsqu'une ACL contient plusieurs règles il faut placer les règles les plus précises en début de liste, et donc les plus génériques en fin de liste.

Algorithme de vérification

- Lorsque le routeur détermine s'il doit acheminer ou bloquer un paquet, la plate-forme logicielle Cisco IOS examine le paquet en fonction de chaque instruction de condition dans l'ordre dans lequel les instructions ont été créées.
- Si le paquet arrivant à l'interface du routeur satisfait à une condition, il est autorisé ou refusé (suivant l'instruction) et les autres instructions ne sont pas vérifiées.
- Si un paquet ne correspond à aucune instruction dans l'ACL, le paquet est jeté. Ceci est le résultat de l'instruction implicite deny any à la fin de chaque ACL.

N


Paquets
Satisfait au premier test
OUI
NON
Satisfait au test suivant
OUI
NON
Satisfait au dernier test
OUI
Autoriser ou refuser
Autoriser (à l'interface de destination)
NON (refus implicite)
Refuser
Elimination

Principe de masque de bits générique

- Un masque générique est une quantité de 32 bits divisés en quatre octets contenant chacun 8 bits.

  - 0 signifie " vérifier la valeur du bit correspondant
  - 1 signifie " ne pas vérifier (ignorer) la valeur du bit correspondant ".

- Les listes de contrôle d'accès utilisent le masquage générique pour identifier une adresse unique ou plusieurs adresses dans le but d'effectuer des vérifications visant à accorder ou interdire l'accès.

- Le terme masque générique est un surnom du procédé de correspondance masque-bit des listes de contrôle d'accès.

Principe de masque de bits générique

- Exemple
  - a- 0.0.255.255 signifie que seuls les 2 premiers octets doivent être examinés.
  - deny 10.1.3.0 avec 0.0.0.255 : refus de toutes les IP commencant par 10.1.3
- On veut vérifier (autoriser ou refuser) les sous réseaux 172.30.16.0 à 172.30.31.0 Les deux premiers octets de l'adresse IP sont identiques.
- 16 en notation binaire: 0001 0000
- 31 en notation binaire: 0001 1111
- Les bits commencent à être différents à partir du 4ème bit de ce 3ème octet. A partir de là on met tous les bits à 1 à Le masque générique est alors 0.0.15.255
- Exemple :
- access-list 1 permit 169.222.30.8 0.0.0.7 → 169.222.30.8 -169,222,30,15

Les commandes host et any

- Ces deux commandes sont des abréviations permettant de simplifier la lecture ainsi que l'écriture des listes de contrôle d'accès :

  - any : n'importe quelle adresse (équivaut à 0.0.0.0 255.255.255.255)

  - host :masque générique d'une adresse d'un hôte

Numérotation des Acl

- Une liste de contrôle d'accès est identifiable par son numéro, attribué suivant le protocole et le type :

Type de liste	Plage de numéros
Listes d'accès standard	1 à 99
Listes d'accès étendues	100 à 199

Les listes de contrôle d'accès standard :

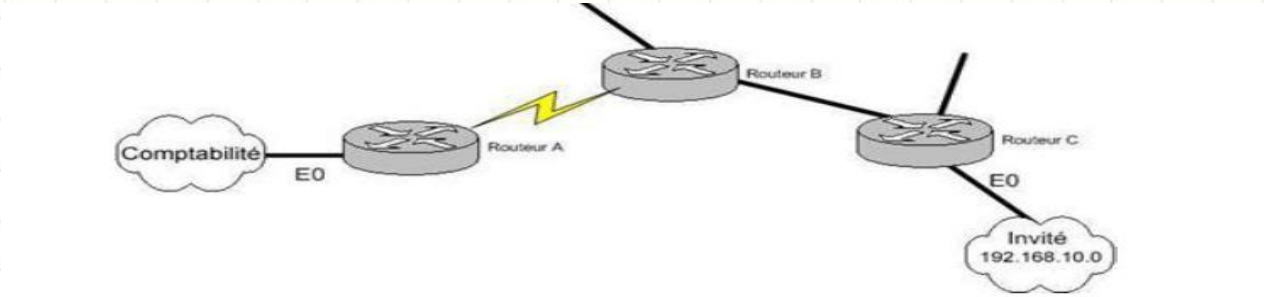
- Une liste d'accès standard se crée par la commande suivante :
  access-list num_acl {permit | deny} source {masque_source}

  - **Numéro_de_liste_d'accès** : identifie la liste
  - **Permit | deny** : autoriser ou interdire
  - **Source** : identifie l'adresse IP source
  - **Masque_source** : bits de masque générique

Exemple :
access-list 1 deny 172.69.0.0 0.0.255.255

Exemple

- Soit la topologie suivante :



- On veut interdire au réseau « Invité 192 .168.10.0» d'accéder au réseau « Comptabilité ».
- Router(config)#access-list 1 deny **192.168.10.0** 0.0.0 .255
- Router(config)#access-list 1 permit **any**
-

Exercice :

- Refuser les paquets d'IP source 172.16.3.10
- Autorise que les trames d'IP source 172.16.3.0/24

Les listes de contrôle d'accès étendues

Une liste de contrôle d'accès étendue permet de faire un filtrage plus précis qu'une liste standard, elle permet également d'effectuer un filtrage en fonction du protocole, du timing, sur le routage… :

Une liste de contrôle d'accès étendue se crée par la commande suivante :

access-list *numéro_de_liste_d'accès {permit | deny} protocole source {masque_source} destination {masque_destination} {opérateur opérande} [established] [log]*

- Numéro_de_liste_d'accès : identifie la liste
- Permit | deny : autoriser ou interdire
- Protocol : indique le type de protocole

o IP, TCP, UDP, ICMP, GRP, IGRP

- Source et destination : identifient l'adresse IP source et destination
- Masque_source et masque_destination : bits de masque générique

- Opérateur :
  - Lt : plus petit
  - Gt : plus grand
  - Eq : égal
  - neq : non égal

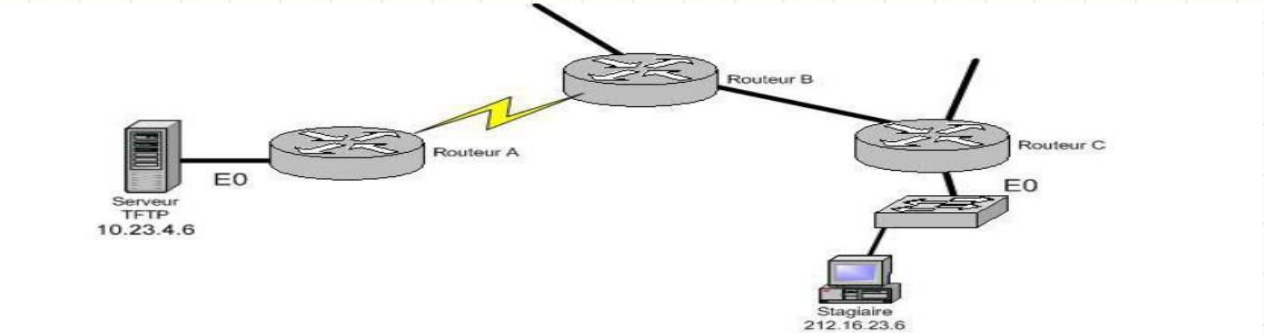
- opérande : n° de port

- established : autorise le trafic TCP si les paquets utilisent une connexion établie (bit de ACK)

Les numéros de ports peuvent être exprimé de manière numérique ou bien par une équivalence alphanumérique

Exemple

- on veut refuser au stagiaire d'adresse : 212.16.23.6 d'accéder au serveur TFTP. d'adresse :10.23.4.10



Assignation d'une liste de contrôle d'accès à une interface

- Une fois la liste de contrôle d'accès crée, il faut l'assigner à une interface de la manière suivante :

Router(config-if)#ip access-group numéro_liste_d'accès {in | out }

- In | out indique si la liste doit être appliquée pour le trafic entrant ou sortant

- Pour vérifier les listes de contrôle d'accès ; La commande **show ip interface** affiche les informations relatives à l'interface IP et indique si des listes de contrôle d'accès sont configurées.

- La commande **show access-lists** affiche le contenu de toutes les listes de contrôle d'accès. La saisie du nom ou du numéro d'une liste de contrôle d'accès en tant qu'option de cette commande vous permet de consulter une liste spécifique

- Assignation d'une liste de contrôle d'accès à une interface *fastEthernet 0/0*
- *R1(config)#interface fastEthernet 0/0*
- *R1(config-if)#ip access-group 101 in*
- *R1(config-if)#exit*