

## Liste de contrôle d'accès

Jean Robert HOUNTOMEY  
hrobert@iservices.tg

Afnog 2007 - Abuja - Nigéria

## Présentation

- Les listes de contrôle d'accès sont des instructions qui expriment une liste de règles supplémentaires sur les paquets reçus et transmis par le routeur.
- Elles peuvent être utilisées pour implémenter la sécurité dans les routeurs
- Les listes de contrôle d'accès sont capables:
  - d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie des interfaces
  - Filtrer le trafic en entrée ou en sortie du routeur
  - Restreinte l'utilisation à des personnes ou à des utilisateurs.
- Elles opèrent selon un ordre séquentiel et logique, en évaluant les paquets à partir du début de la liste d'instructions.

Afnog 2007 - Abuja - Nigéria

## Présentation

Si le paquet répond au critère de la première instruction, il ignore le reste des règles et il est autorisé ou refusé.

- L'ACL s'exécute dans la direction indiquée par le mot IN ou OUT
- A un deny implicite à la fin. Aussi si le paquet ne satisfait à aucune règle il est rejeté.

Afnog 2007 - Abuja - Nigéria

## 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 IP standard	1 à 99 et 1300 à 1999
Listes d'accès IP étendues	100 à 199 et 2000 à 2699
Listes d'accès Appletalk	600 à 699
Listes d'accès IPX standard	800 à 899
Listes d'accès IPX étendues	900 à 999
Listes d'accès IPX SAP	1000 à 1099

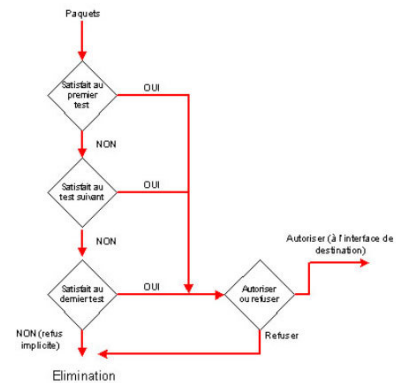
NB: On s'intéressera seulement aux acl IP

Afnog 2007 - Abuja - Nigéria

## 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.

Afnog 2007 - Abuja - Nigéria



Afnog 2007 - Abuja - Nigéria

### Principe de masque de bits générique - WILCARD

- 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.

Afnog 2007 - Abuja - Nigéria

### Principe de masque de bits générique - WILCARD

- 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.

Afnog 2007 - Abuja - Nigéria

### Principe de masque de bits générique - WILCARD

- Entre d'autres termes le WILCARD est l'inverse du NETMASK.

#### Exemples:

- Pour spécifier une machine:
  - **196.200.221.1 0.0.0.0**
- Pour spécifier un sous réseau
  - 196.200.221.8 - 196.200.221.15 (would be a /29)
  - Le bloc deviens **196.200.221.8 0.0.0.7**
- Pour spécifier tous les hosts d'un réseau /24
  - **196.200.220.1 0.0.0.255**

Afnog 2007 - Abuja - Nigéria

### 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 (équivalent à 0.0.0.0 255.255.255.255)

- **host** : abréviation du masque générique  
Ex: host 172.16.33.5 équivalent à 172.16.33.5 255.255.255.255

Afnog 2007 - Abuja - Nigéria

### Nommage des Acl

- Depuis la version 11.2 d'IOS, il est possible d'utiliser les listes de contrôles d'accès nommées.
- Les listes de contrôle d'accès nommées permettent d'identifier les listes de contrôle d'accès IP standards et étendues par des chaînes alphanumériques plutôt que par la représentation numérique actuelle.
- Vous pouvez utiliser les listes de contrôle d'accès nommées dans les situations suivantes :
  - Identifier intuitivement les listes de contrôle d'accès à l'aide d'un code alphanumérique.
  - Configurer plusieurs ACL standard et plusieurs ACL étendues dans un routeur pour un protocole donné

Afnog 2007 - Abuja - Nigéria

### Syntaxe des Acl

#### IP Access List standard Configuration Syntax

- **access-list access-list-number {permit | deny} source {source-mask}**
- **ip access-group access-list-number {in | out}**

#### IP Access List Etendu Configuration Syntax

- **access-list access-list-number {permit | deny} protocol source {source-mask} destination {destination-mask}**
- **ip access-group access-list-number {in | out}**

#### IP Access List Nommé Configuration Syntax

- **ip access-list {standard | extended} {name | number}**

Afnog 2007 - Abuja - Nigéria

## Placer les ACL

Placer les ACL standard proche de la destination  
**Standard IP access list close to destination**

Place les ACL étendus proche de la source du trafic à gérer

Afnog 2007 - Abuja - Nigéria

## Appliquer les ACL

Une fois la liste de contrôle d'accès créée, 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

Afnog 2007 - Abuja - Nigéria

Permettre seulement à mon réseau interne de faire du telnet

```
access-list 1 permit 196.200.221.192 0.0.0.15
access-list 1 deny any
line vty 0 4
  access-class 1 in
```

Afnog 2007 - Abuja - Nigéria

## Prefix Lists

- Cisco introduit les prefix lists dans l'IOS 12.0
- Utilisés pour filter les routes et peuvent être combinés avec des route maps
- Donne des fonctionnalités élevées par rapport aux ACL
- Plus simples à configurer et à utiliser
  - Utilise la notation CIDR address/mask
  - Numéros de Sequence

Afnog 2007 - Abuja - Nigéria

## Prefix Lists

- Prefix lists ont un implicite "deny" à la fin comme les ACL
- Sont plus rapides à exécuter que les ACL
- Prédéférables si IOS 12.0 pour les manipulations de routes

Afnog 2007 - Abuja - Nigéria

## Syntaxe de Configuration d'une Prefix List

- Prefix list configuration syntax
  - **config t**  
**ip prefix-list list-name {seq seq-value} {permit|deny} network/len {ge ge-value} {le le-value}**
  - **list-name** - nom de la liste
  - **seq-value** - numéro de séquence (optionnelle)
  - **network/len** - CIDR
  - **ge-value** - "from" valeur de la plage; matches égale ou préfixes plus longs (plus de bits dans le préfixe, bloc plus petit)
  - **le-value** - "to"; matches égale ou préfixes plus petits (moins de bits dans le préfixe, blocs plus larges)

Afnog 2007 - Abuja - Nigéria

## Prefix List Configuration

- Pour interdire un /28:  
**ip prefix-list f2afnog seq 5 deny 196.200.221.192/28**
- Pour accepter les préfixes de /8 à /24:  
**ip prefix-list test1 seq 5 permit 196.0.0.0/8 le 24**
- Refuser les préfixes aec un masque plus grand que /25 dans un bloc  
**ip prefix-list test2 seq 10 deny 196.200.221.0/24 ge 25**
- Permettre toutes les routes:  
**ip prefix-list test3 seq 15 permit 0.0.0.0/0 le 32**

Afnog 2007 - Abuja - Nigéria