Liste de contrôle d'accès

Jean Robert HOUNTOMEY
hrobert@iservices.tg

Présentation

- Les listes de contrôle d'accès sont des instructions qui expriment une liste de règles, imposées par l'opérateur, donnant un contrôle supplémentaire sur les paquets reçus et transmis par le routeur.
- Les listes de contrôle d'accès sont capables d'autoriser ou d'interdire des paquets, que ce soit en entrée ou en sortie vers une destination.
- Elles opèrent selon un ordre séquentiel et logique, en évaluant les paquets à partir du début de la liste d'instructions. Si le paquet répond au critère de la première instruction, il ignore le reste des règles et il est autorisé ou refusé.

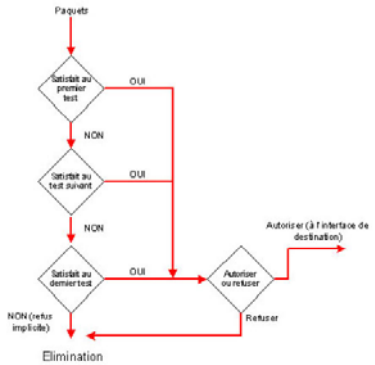
Numérotation des Acl

- 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
Listes d'accès IP étendues	100 à 199
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

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.



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.

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 : abréviation du masque générique
  Ex: host 172.16.33.5 équivaut à 172.16.33.5 255.255.255.255

LES DIFFÉRENTS TYPES DE LISTES DE CONTRÔLE D'ACCÈS

Les listes de contrôle d'accès standard :

- Les listes de contrôle d'accès standard permettent d'autoriser ou d'interdire des adresses spécifiques ou bien un ensemble d'adresses ou de protocoles
- 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

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 :
  - o Lt : plus petit
  - o Gt : plus grand
  - o Eq : égal
  - o 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

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 ACLétendues dans un routeur pour un protocole donné

- Pour configurer les listes de contrôle d'accès nommées, la syntaxe est la suivante :
  Router(config)# ip access-list {**standard | extended**} nom

  En mode de configuration de liste de contrôle d'accès, précisez une ou plusieurs conditions d'autorisation ou de refus. Cela détermine si le paquet est acheminé ou abandonné.
  Router (config {std- | ext-}nacl)# deny *{source [masque-générique-source] |* ***any****}*
  ou
  Router (config {std- | ext-}nacl)# permit *{source [masque-générique-source] |* ***any****}*

  La configuration illustrée dans la figure crée une liste de contrôle d'accès standard nommée *Internetfilter* et une liste de contrôle d'accès étendue nommée afnog_*group*.

```
Ip interface ethernet0/1
Ip address 2.0.5.1.255.255.255.0
Ip address-group Internetfilter out
Ip access-group afnog_group in
...

ip access-list standard Internetfilter
permit 1.2.3.4
deny any

ip access-list extended afnog_group
permit tcp any 171.69.0.0.0.255.255.255 eq telnet
deny tcp any any
deny udp any 171.69.0.0.0.255.255.255 lt 1024
deny ip any log
```


L'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

Emplacement des ACL

- La règle est de placer les listes de contrôle d'accès étendues le plus près possible de la source du trafic refusé. Étant donné que les listes de contrôle d'accès standard ne précisent pas les adresses de destination, vous devez les placer le plus près possible de la destination.
- Pour tirer parti des avantages des listes de contrôle d'accès en matière de sécurité, vous devez au moins configurer des listes de contrôle d'accès sur les routeurs périphériques situés aux frontières du réseau. Cela permet de fournir une protection de base contre le réseau externe ou de mettre à l'abri une zone plus privée du réseau d'une zone moins contrôlée.
- Sur ces routeurs périphériques, des listes de contrôle d'accès peuvent être créées pour chaque protocole réseau configuré sur les interfaces des routeurs. Vous pouvez configurer des listes de contrôle d'accès afin que le trafic entrant, le trafic sortant ou les deux soient filtrés au niveau d'une interface.