



ACL : Access-list

>>> Pour équipements Cisco

Description :

Les ACL (Access Control Lists) permettent de filtrer des paquets suivant des critères définis par l'utilisateur.

ACL : Access-list

>>> Pour équipements Cisco

Sommaire :

- I) Les ACL Cisco
 - II) Fonctionnement et configuration
 - 1) La logique des ACL
 - 2) Standard IP Access List Configuration
 - 3) Exemple ACL standard
 - 4) Exemple d'interdiction de machine
 - 5) Exemple
 - 6) Les ACL étendue
 - 7) Exemple de syntaxe
 - 8) Les ACL nommées
 - III) Quelques conseils
-

I) Les ACL Cisco

Sur des paquets IP, il est ainsi possible de filtrer les paquets entrants ou sortants d'un routeur en fonction :

- De l'IP source
- De l'IP destination

Il existe 2 types d'ACL :

- Standard : uniquement sur les IP sources
- Étendue : sur quasiment tous les champs des en-têtes IP, TCP et UDP

II) Fonctionnement et configuration

1) La logique des ACL

Il est possible de résumer le fonctionnement des ACL de la façon suivante :

- Le paquet est vérifié par rapport au 1er critère défini
- S'il vérifie le critère, l'action définie est appliquée
- Sinon le paquet est comparé successivement par rapport aux ACL suivants
- S'il ne satisfait aucun critère, l'action deny est appliquée

Les critères sont définis sur les informations contenues dans les en-têtes IP, TCP ou UDP

Des masques ont été définis pour pouvoir identifier une ou plusieurs adresses IP en une seule définition

- Ce masque définit la portion de l'adresse IP qui doit être examinée
- 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 commençant par 10.1.3

2) Standard IP Access List Configuration

Fonctionnement des ACL :

- Test des règles les unes après les autres.
- Si aucune règle n'est applicable, rejet du paquet.

Définition d'une règle :

```
access-list number [deny|permit] source [source-wildcard]
```

Number compris entre 1 et 99 ou entre 1300 et 1999

```
access-list number remark test
```

Activation d'une ACL sur une interface :

```
ip access-group [ number | name [ in | out ] ]
```

Visualiser les ACL :

show access-lists number : toutes les ACL quelque soit l'interface.

show ip access-lists number : les ACL uniquement liés au protocole IP.

3) Exemple ACL standard

```
Switch# configure terminal
Switch(config)# access-list 1 remark stop tous les paquets d'IP source 172.16.3.10
Switch(config)# access-list 1 deny 172.16.3.10 0.0.0.0
Switch(config)# access-list 1 permit 0.0.0.0 255.255.255.255
Switch(config)# interface fastethernet0
Switch(config-if)# ip address 172.16.1.1 255.255.255.0
Switch(config-if)# ip access-group 1 out
```

```
access-list 1 deny 172.16.3.10 0.0.0.0
```

- Refuse les paquets d'IP source 172.16.3.10.

- Le masque (également appelé wildcard mask) signifie ici que tous les bits de l'adresse IP sont significatifs.

```
access-list 1 permit 0.0.0.0 255.255.255.255
```

- Tous les paquets IP sont autorisés.

- Le masque 255.255.255.255 signifie qu'aucun bit n'est significatif.

4) Exemple d'interdiction de machine

```
Switch# configure terminal
Switch(config)# access-list 1 remark stop tous les paquets d'IP source 172.16.3.10
Switch(config)# access-list 1 deny host 172.16.3.10
Switch(config)# access-list 1 permit any
Switch(config)# interface fastethernet0
Switch(config-if)# ip address 172.16.1.1 255.255.255.0
Switch(config-if)# ip access-group 1 out
```

Une notation améliorée est possible pour remplacer :

- le masque 255.255.255.255 qui désigne une machine.

=> Utilisation du terme **host**

- 0.0.0.0 avec le wildcard masque à 255.255.255.255 qui désigne tout le monde.

=> Utilisation du terme **any**

5) Exemple

```
Switch# configure terminal
Switch(config)# access-list 1 remark Stoppe tous les paquets d'IP source 172.16.3.10
Switch(config)# access-list 1 deny host 172.16.3.10
Switch(config)# access-list 1 permit any
Switch(config)# access-list 2 remark Autorise que les trames d'IP source 172.16.3.0/24
Switch(config)# access-list 2 permit 172.16.3.0 0.0.0.255
Switch(config)# interface fastethernet0
Switch(config-if)# ip address 172.16.1.1 255.255.255.0
Switch(config-if)# ip access-group 1 out
Switch(config)# exit
Switch(config)# interface fastethernet1
Switch(config-if)# ip address 172.16.2.1 255.255.255.0
Switch(config-if)# ip access-group 2 in
```

6) Les ACL étendue

Les extended ACL permettent de filtrer des paquets en fonction :

- De l'adresse de destination IP
- Du type de protocole (TCP, UDP, ICMP, IGRP, IGMP, ...)
- Port source
- Port destination
- ...

7) Exemple de syntaxe

```
access-list number { deny | permit } protocol source source-wildcard destination dest.-wildcard
```

- **number** : compris entre 100 et 199 ou 2000 et 2699

```
access-list 101 deny ip any host 10.1.1.1
```

- Refus des paquets IP à destination de la machine 10.1.1.1 et provenant de n'importe quelle source

```
access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23
```

- Refus de paquet TCP provenant d'un port > 1023 et à destination du port 23 de la machine d'IP 10.1.1.1

```
access-list 101 deny tcp any host 10.1.1.1 eq http
```

- Refus des paquets TCP à destination du port 80 de la machine d'IP 10.1.1.1

8) Les ACL nommées

- Une ACL numérotée peut être composée de nombreuses règles. La seule façon de la modifier et de faire :

```
no access-list number
```

- Puis de la redéfinir

- Avec les ACL nommées, il est possible de supprimer qu'une seule ligne au lieu de toute l'ACL
- Sa définition se fait de la manière suivante

```
Router(config)# ip access-list extended bart  
Router(config-ext-nacl)# deny tcp host 10.1.1.2 eq www any  
Router(config-ext-nacl)# deny ip 10.1.1.0 0.0.0.255 any  
Router(config-ext-nacl)# permit ip any any
```

- Pour supprimer une des lignes, il suffit de refaire un :

```
ip access-list extended bart  
no deny ip 10.1.1.0 0.0.0.255 any
```

III) Quelques conseils

La création, la mise à jour, le debuggage nécessitent beaucoup de temps et de rigueur dans la syntaxe

Il est donc conseillé :

- De créer les ACL à l'aide d'un éditeur de texte et de faire un copier/coller dans la configuration du routeur
- Placer les extended ACL au plus près possible de la source du paquet pour le détruire le plus vite possible
- Placer les ACL standard au plus près de la destination sinon, vous risquez de détruire un paquet trop tôt.

Rappel : les ACL standard ne regardent que l'IP source

- Placer la règle la plus spécifique en premier.
- Avant de faire le moindre changement sur une ACL, désactivez celle-ci sur l'interface concerné (**no ip access-group**).



Idum