# ACL – Access Control List

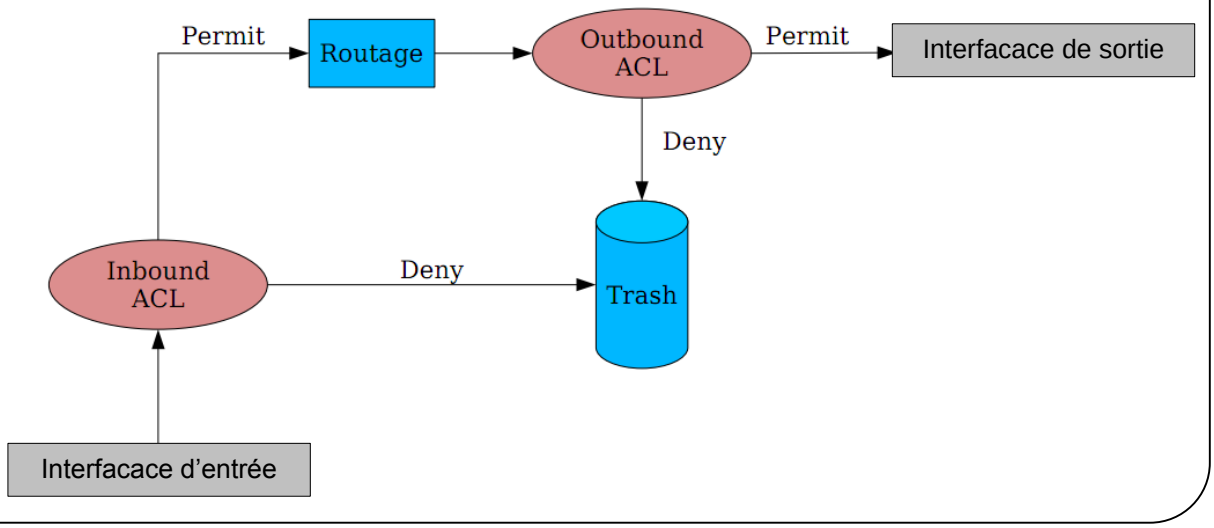


## Généralités

- Une ACL est une liste de règles permettant de filtrer ou d'autoriser du trafic sur un réseau en fonction de certains critères (IP source, IP destination, port source, port destination, protocole, …).
- Une ACL permet de soit autoriser du trafic (permit) ou de le bloquer (deny).
- Il est possible d'appliquer au maximum une ACL par interface et par sens (input/output).
- Une ACL est analysée par l'IOS de manière séquentielle.
- Dès qu'une règle correspond au trafic, l'action définie est appliquée, le reste de l'ACL n'est pas analysé.
- Toute ACL par défaut bloque tout trafic. Donc tout trafic ne correspondant à aucune règle d'une ACL est rejeté.

Remarque: Les ACLs servent également à identifier un trafic afin d'être traité par un processus, dans ce cas le trafic correspondant à un « permit » est traité, et celui correspondant à un « deny » est ignoré.

## Les ACLs et le routage




## ACL Standard

Permet d'analyser du trafic en fonction de:

- Adresse IP source

Les ACLs standard sont à appliquer le plus proche possible de la destination en raison de leur faible précision.

## ACL Etendues

Permet d'analyser du trafic en fonction de:

- Adresse IP source
- Adresse IP destination
- Protocole (tcp, udp, icmp, …)
- Port source
- Port destination
- Etc.

Les ACLs étendues sont à appliquer le plus proche possible de la source.

## 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.

## Conseils

- Concevoir une ACL dans un éditeur de texte et la configurer par copier/coller.
- Désactiver une ACL sur une interface avant de la modifier.

# ACL – Access Control List

## Configuration d'une ACL numérique standard

```
R1(config)#access-list 1 permit 192.168.0.0 0.0.0.255
R1(config)#access-list 1 permit 192.168.1.0 0.0.0.255
R1(config)#access-list 1 deny 192.168.0.0 0.0.3.255
R1(config)#access-list 1 permit any
```

## Configuration d'une ACL nommée standard

```
R1(config)#ip access-list standard monACL
R1(config-std-nacl)#permit 192.168.0.0 0.0.0.255
R1(config-std-nacl)#permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)#deny 192.168.0.0 0.0.3.255
R1(config-std-nacl)#permit any
R1(config-std-nacl)#exit
```

## Vérification des ACLs

```
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Standard IP access list monACL
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
R1#
```

Ces deux ACLs sont identiques.
Tout le trafic provenant du réseau 192.168.0.0/22 est bloqué à l'exception des deux subnets 192.168.0.0/24 et 192.168.1.0/24.

### ACL « numériques »

ACL identifées par un nombre.

| | |
|---|---|
| 1 à 99 : | ACL Standard |
| 100 à 199 : | ACL Etendue |
| 1300 à 1999 : | ACL Standard |
| 2000 à 2699 : | ACL Etendue |

### ACL « nommées »

ACL identifiées par un nom sous la forme d'une chaîne de caractères alphanumériques.

## Configuration d'une ACL numérique étendue

```
R1(config)#access-list 100 permit tcp any host 192.168.1.100 eq 80
R1(config)#access-list 100 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
```

## Configuration d'une ACL nommée étendue

```
R1(config)#ip access-list extended monACLextended
R1(config-ext-nacl)#permit tcp any host 192.168.1.100 eq 80
R1(config-ext-nacl)#permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
R1(config-ext-nacl)#exit
```

## Vérification des ACLs

```
R1#show access-lists
Extended IP access list 100
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list monACLextended
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
R1#
```

Ces deux ACLs sont identiques.
- Tout trafic HTTP à destination de 192.168.1.100 est autorisé.
- Tout le traffic ICMP provenant de 192.168.0.0/24 à destination de 192.168.1.100 est autorisé.
- Tout autre trafic est rejeté.

## Format général d'une règle étendue

```
<action> <protocole> <IP source> [port source] <IP dest> [port dest] [options]
```

- **<action>** : Permit / deny
- **<protocole>** : Tcp / udp , … Ip = tous les protocoles
- **<IP source>** : Adresse + wildcard mask. Ou Host 192.168.0.1 (adresse d'un hôte) Ou Any = n'importe quelle source.
- **<IP dest>** : Adresse + wildcard mask. Ou Host 192.168.0.1 (adresse d'un hôte) Ou Any = n'importe quelle source.

## Modifier une ACL

```
R1#show access-list 1
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
R1#configure terminal
R1(config)#ip access-list standard 1
R1(config-std-nacl)#no 20
R1(config-std-nacl)#15 permit 192.168.1.0 0.0.0.127
R1(config-std-nacl)#^Z
R1#show access-list 1
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    15 permit 192.168.1.0, wildcard bits 0.0.0.127
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
R1#
```

Entre en mode de configuration d'ACL

Supprime la règle portant le n° de séquence 20

Ajoute une régle avec le n° de séquence 15

## Supprimer une ACL

```
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    15 permit 192.168.1.0, wildcard bits 0.0.0.127
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Standard IP access list monACL
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    20 permit 192.168.1.0, wildcard bits 0.0.0.255
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Extended IP access list 100
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list monACLextended
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list test
R1#configure terminal t
R1(config)#no access-list 100
R1(config)#no ip access-list standard monACL
R1(config)#^Z
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.0.0, wildcard bits 0.0.0.255
    15 permit 192.168.1.0, wildcard bits 0.0.0.127
    30 deny   192.168.0.0, wildcard bits 0.0.3.255
    40 permit any
Extended IP access list monACLextended
    10 permit tcp any host 192.168.1.100 eq www
    20 permit icmp 192.168.0.0 0.0.0.255 host 192.168.1.100
Extended IP access list test
R1#
```

Suppression d'une ACL numérotée

Suppression d'une ACL nommée

## Appliquer une ACL sur une interface

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 1 in
              OU
R1(config-if)#ip access-group 1 out
R1(config-if)#
```

Applique l'ACL 1 pour le trafic entrant sur l'interface

Applique l'ACL 1 pour le trafic sortant de l'interface

## Vérification des ACLs appliquées sur une interface

```
R1#show ip interface fastEthernet 0/0
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is 1
  Inbound  access list is 1
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  < … suite de l'affichage omis … >
R1#
```

ACL 1 appliquée en sortie

ACL 1 appliquée en entrée

## Désactiver une ACL sur une interface

```
R1(config)#interface fastethernet 0/0
R1(config-if)#no access-group 1 in
              OU
R1(config-if)#no access-group 1 out
R1(config-if)#
```

## Appliquer une ACL sur les lignes VTY

```
R1(config)#line vty 0 4
R1(config-if)#access-class 1 in
R1(config-if)#
```

## Désactiver une ACL sur les lignes VTY

```
R1(config)#line vty 0 4
R1(config-if)#no access-class 1 in
R1(config-if)#
```

## Vérifier le fonctionnement d'une ACL

```
R1#show access-lists workingACL
Extended IP access list workingACL
    10 permit tcp any host 193.190.147.70 eq www (2 matches)
    20 permit icmp any host 193.190.147.70 (14 matches)
    30 deny ip any host 193.190.147.70 (4926 matches)
    40 permit ip any any (878382 matches)
R1#
```

Indique le nombre de fois où une règle de l'ACL a été appliquée