Liste de contrôle d'accès d'un routeur Cisco

I Présentation

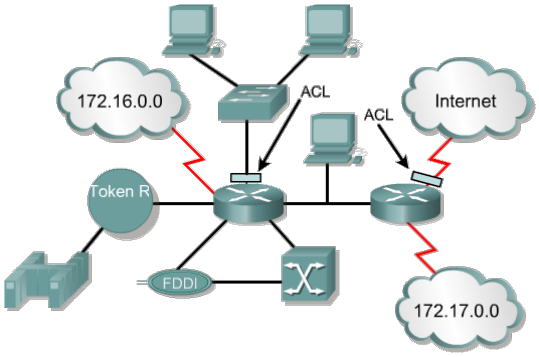
Un réseau doit être protégé contre les attaques de pirates informatiques. Cela signifie que les accès au réseau en provenance extérieure de celui-ci doit être limités aux seuls accès autorisés. Il faut mettre ne place pour cela, un pare-feu

Dans les routeurs Cisco, la technique de base pour limiter ou interdire les accès à un système est l'utilisation d'ACL : **Liste de contrôle d'Accès** (Access Control List).

Définition :

Une liste de contrôle d'accès est une collection d'instructions permettant d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères, tels que :

- L'adresse d'origine ;
- L'adresse de destination ;
- Le numéro de port ;
- Les protocoles de couches supérieures ;
- D'autres paramètres (horaires par exemple).



Elles définissent des conditions en entrée et en sortie de chaque interface du routeur.

Voici les principales raisons pour lesquelles il est nécessaire de créer des listes de contrôle d'accès :

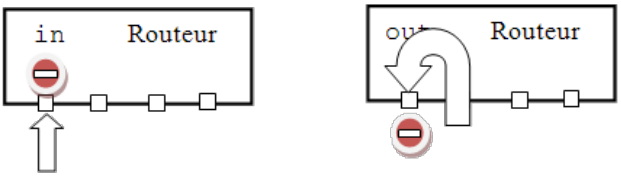
- Limiter le trafic réseau et accroître les performances. En limitant le trafic vidéo, par exemple, les listes de contrôle d'accès permettent de réduire considérablement la charge réseau et donc d'augmenter les performances.
- Contrôler le flux de trafic. Les ACL peuvent limiter l'arrivée des mises à jour de routage. Si aucune mise à jour n'est requise en raison des conditions du réseau, la bande passante est préservée.
- Fournir un niveau de sécurité d'accès réseau de base. Les listes de contrôle d'accès permettent à un hôte d'accéder à une section du réseau tout en empêchant un autre hôte d'avoir accès à la même section. Par exemple, l'hôte A peut accéder au réseau réservé aux ressources humaines, tandis que l'hôte B ne peut pas y accéder.
- Déterminer le type de trafic qui sera acheminé ou bloqué au niveau des interfaces de routeur. Il est possible d'autoriser l'acheminement des messages électroniques et de bloquer tout le trafic via Telnet.
- Autoriser un administrateur à contrôler les zones auxquelles un client peut accéder sur un réseau.
- Filtrer certains hôtes afin de leur accorder ou de leur refuser l'accès à une section de réseau. Accorder ou refuser aux utilisateurs la permission d'accéder à certains types de fichiers, tels que FTP ou HTTP.

II Principe

Pour un paquet donné, l'ACL prend deux valeurs :

- **deny** : le paquet sera rejeté
- **permit** : le paquet pourra transiter par le routeur

On associe à chaque interface du routeur une ACL. On peut aussi préciser le sens du trafic, c'est-à-dire in ou out, pour que l'ACL s'applique aux paquets entrant ou sortant de l'interface du routeur.

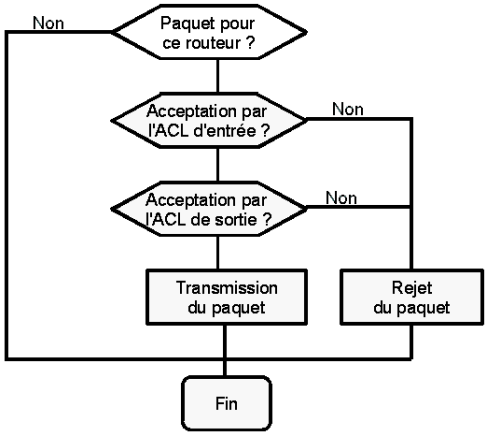


L'ordre des instructions ACL est important. Les règles sont parcourues séquentiellement et le test s'arrête lorsque le paquet testé vérifie une règle. En général, on essaie de mettre les règles les plus utilisées en début de liste.

Si aucune règle n'est vérifiée, le résultat sera négatif (deny) : tout ce qui n'est pas autorisé est interdit.

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

- ✗ Le paquet est vérifié par rapport au premier 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 sera appliquée.



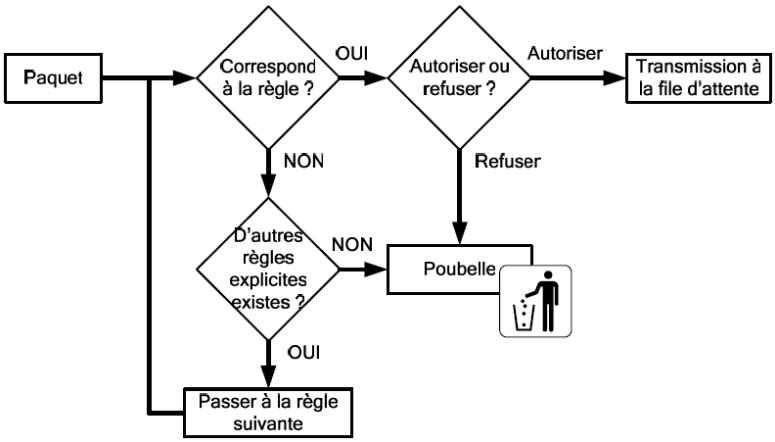
Une liste ACL est donnée pour chaque entrée ou sortie d'une interface et pour chaque protocole de couche 3. Quand un accès au routeur est effectué, la liste d'entrée correspondante à l'interface et à la couche est analysée si elle existe. Si la liste n'existe pas ou si le paquet est acceptée par la première liste, la liste de sortie correspondante à l'interface et à la couche est également analysée. Si cette liste existe et si elle accepte le paquet ou si la liste n'existe pas, le paquet est transmis.

Bien sûr, seuls les paquets concernant le routeur en question sont traités.

Chaque contrôle d'accès peut être de deux types :

- ✗ Acceptation : **permit** ;
- ✗ Rejet : **deny**.

Quand la ligne est trouvée, si le contrôle est **permit** l'accès est autorisé. Si le contrôle est **deny**, le paquet est rejeté.



Il existe deux types de contrôle pour le protocole IP :

- **ACL IP standard** :
  - Travail sur la source (de quelle interface les données sont transmises) ;
  - Filtrage sur le masque (selon les adresses réseau) ;
  - Un numéro unique de liste compris entre 1-99 ou 1300-1999.
  - **Règle** : liste à appliquer au plus près de la destination (interface vers laquelle les données seront envoyées).
- **ACL IP étendu** :
  - Travail sur les adresses IP et le port de la source et de la destination ;
  - Filtrage sur la couche 4 (port et adresse IP) ;
  - Un numéro unique de liste compris entre 100-199, 2000-2699.
  - **Règle** : liste à appliquer au plus près de la source.

Les ACL pour les protocoles IPX et AppleTalk ne sont pas étudiées.

Il existe un troisième type d'ACL appelés ACL nommés. Ces ACL sont de type standard ou étendu. Leur seule particularité est l'ajout d'un nom pour une plus grande lisibilité.

Le numéro unique de liste identifie le type de liste d'accès créé et doit être compris dans la plage de numéros valide pour ce type.

III Règle générale

La règle générale est de placer les listes de contrôle d'accès étendu le plus près possible de la source du trafic refusé afin de le détruire le plus vite possible.

Étant donné que les listes de contrôle d'accès standard ne précise pas les adresses de destination, on doit les placer le plus près possible de la destination afin de ne pas de détruire le paquet trop tôt.

Il faut placer la règle la plus spécifique en premier.

Il est conseillé de créer les ACL à l'aide d'un éditeur de texte et de faire un copier/coller dans la configuration du routeur.

Il faut désactiver l'ACL sur l'interface concernée (no ip access-group) avant de faire le moindre changement sur une ACL.

IV L'édition des ACL

Pour saisir les instructions des ACL, il faut entrer la commande access-list dans le mode de configuration globale.

Exemple :

```
Router#configure terminal
Router(config)#access-list 101 permit tcp any any established
Router(config)#access-list 101 deny ip any host 172.16.0.1
```

Le premier paramètre de la commande access-list définit le numéro de la liste. Il suffit d'entrer dans l'ordre les différentes lignes de votre ACL en respectant le format de la commande.

Dans l'exemple ci-dessus, tous les paquets concernant une connexion TCP établie (réponse à une requête) sont autorisés, tous les paquets à destination de la machine 172.16.0.1 sont rejetés.

Après avoir créé votre liste, vous devez indiquer au routeur que cette liste doit être appliquée à quelle interface et si elle est en entrée (in) ou en sortie (out) par la commande **ip access-group <numéro> <in ou out>**.

```
Router#configure terminal
Router(config)#interface fa0/0
Router(config-if)#ip access-group 101 in        Filtrage des paquets entrants via fa0/0
Router(config-if)#exit
Router(config)#exit
```

La liste 101 est appliquée en entrée de l'interface fa0/0.

Si vous voulez visualiser l'ensemble des lignes de votre ACL, il faut utiliser la commande « **show access-list <numéro>** ».

```
Router#sh access-lists
Extended IP access list 101
  10 permit ip 192.168.1.32 0.0.0.15 any (55 matches)
  20 deny ip any any (505 matches)
Extended IP access list 102
  10 permit tcp any any established
  20 permit icmp any any echo-reply
  30 permit icmp any any unreachable
  40 deny ip any any
```

On a visualisé les deux listes 101 et 102, la liste 101 applique d'abord la règle acceptant tous la paquets ayant pour adresse source 192.168.1.32 à 192.168.1.63, tous les autres paquets sont rejetés.

Attention : Si suite à cette visualisation, vous remarquez une ligne manquante ou incorrecte, vous ne pouvez pas modifier l'ordre de votre liste. Vous devez supprimer la liste par la commande **no access-list <numéro>** puis entrer à nouveau votre liste.

```
Router#configure terminal
Router(config)#no access-list 101
```

Une solution pour éviter de retaper toute la liste est de créer un fichier contenant cette liste puis d'utiliser le copier-coller pour entrer la liste.

Si vous ne voulez que retirer une ligne, vous pouvez le faire :

```
Router#show access-list
Extended IP access list 125
    10 permit icmp 10.x.x.x 0.0.0.255 any
    20 permit icmp 20.x.x.x 0.0.0.255 any
    30 permit icmp 30.x.x.x 0.0.0.255 any
Router#conf t
Router(config)#ip  access-list  extended  125
Router(config-ext-nacl)#no  permit  icmp  10.x.x.x  0.0.0.255  any
Router#sh access-lists
Extended IP access list 125
    20 permit icmp 20.x.x.x 0.0.0.255 any
    30 permit icmp 30.x.x.x 0.0.0.255 any
```

Exemple de fichier liste :

```
no access-list 101
access-list 101 permit tcp any host 172.16.0.1 eq www
access-list 101 deny ip any host 172.16.0.1
access-list 101 permit ip 172.171.3.192 0.0.0.63 209.0.0.128 0.0.0.127
access-list 101 deny ip any 209.0.0.128 0.0.0.127
access-list 101 permit ip 172.171.3.128 0.0.0.127 209.0.0.0 0.0.0.127
access-list 101 deny ip any 209.0.0.0 0.0.0.127
access-list 101 deny ip any host 198.0.0.1
access-list 101 permit ip any any
```

Vous pouvez également visualiser les ACL prises en compte sur une interface en utilisant la commande :

```
show ip interface <interface>
```

Exemple :

```
Router#show ip interface fa0/0
...
Outgoing access list is not set
```

```
Inbound access list is 102
...
```

Pour l'interface fa0/0, la liste 102 est appliquée en entrée.

Les commandes access-list sont différentes selon le type de liste (standard ou étendu). Mais il faut d'abord étudier les masques génériques.

V Les masques génériques

Un masque générique est une quantité de 32 bits divisés en quatre octets. Il est associé à une adresse IP. Il permet de déterminer quelles sont les adresses IP concernées par le contrôle.

Attention : le masque est différent du masque de sous-réseau.

Les 0 indiquent qu'il faut tester ces bits et les 1 qu'aucun test n'est à effectuer.

Dans la majorité des cas, le masque générique est simplement l'inverse du masque réseau, c'est-à-dire les 1 sont remplacés par des 0 et vice-versa.

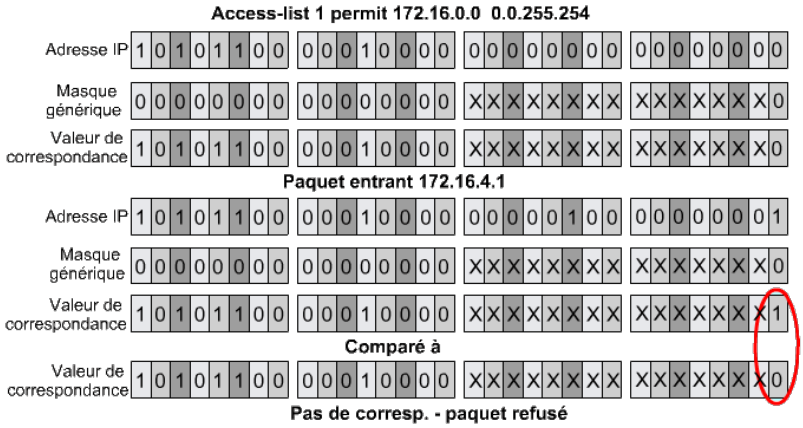
Par exemple, si vous voulez accepter les paquets provenant du réseau 192.168.0.128/23 (masque 255.255.255.128), vous devez utiliser le masque 0.0.0.127.

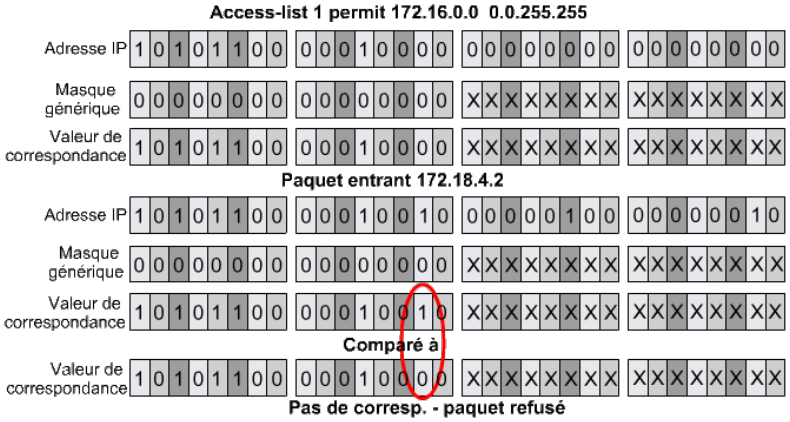
Mais si vous voulez appliquer sur quelques adresses d'un réseau vous devrez utiliser un masque un peu plus compliqué.

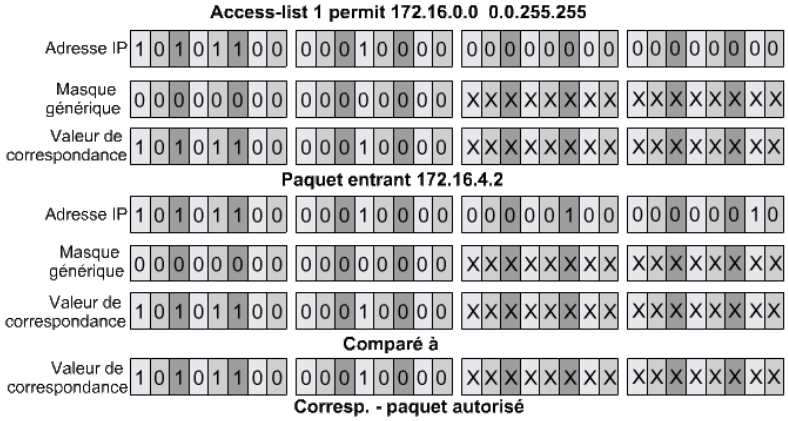
Pour vérifier si une adresse IP appartient à une famille d'adresse IP à analyser :

- ✗ Prendre l'adresse IP ;
- ✗ Appliquer le masque, c'est-à-dire mettre à 0 dans l'adresse IP tous les bits qui sont à 1 dans le masque ;
- ✗ Comparer le résultat obtenu à l'adresse générique de la famille.

Voici quelques exemples :







Exemple : contrôle concernant les sous-réseaux 172.30.16.0 à 172.30.31.0

172.30.16.0 en binaire : 1010 1100.0001 1110.0001 0000.0000 0000

172.30.31.0 en binaire : 1010 1100.0001 1110.0001 1111.0000 0000

Les bits différents sont mis à 1 : 0000 0000.0000 0000.0000 1111.0000 0000

Pour prendre en compte les adresses hôtes du sous-réseau : il faut remplacer le dernier octet par 1111 1111.

On obtient donc : 0000 0000.0000 0000.0000 1111.1111 1111 soit 0.0.15.255.

Il existe deux masques particuliers :

- 255.255.255.255 qui correspond à toutes les adresses peut être remplacé par **any**.
- 0.0.0.0 qui correspond à l'adresse exacte peut être remplacé par **host**.

VI Les ACL standard

Les listes d'accès standard vérifient l'adresse d'origine des paquets IP qui sont routés, pour accepter ou rejeter les paquets.

Les commandes pour les ACL standard sont de la forme :

```
access-list <numéro d'ACL> {deny | permit} <adresse d'origine> <masque générique>
```

- **deny** : rejet du paquet
- **permit** : acceptation du paquet
- **adresse d'origine** et **masque générique** : déterminent les adresses IP concernées par ce contrôle.

Exemple :

```
Router(config)#access-list 1 deny 192.168.14.0   0.0.0.255      L'accès au réseau
192.168.14.0 est refusé.
Router(config)#access-list 1 permit any        Tous les autres accès sont permis.
Router(config)#int fa0/0
Router(config-if)#ip access-group 1 in         Application la liste d'accès 1 en entrée
sur l'interface fa0/0
Router(config-if)#exit
```

VII Les ACL étendues

Les listes d'accès étendues vérifient les adresses d'origine et de destination du paquet, mais peuvent aussi vérifier les protocoles et les numéros de port. Les commandes pour les ACL étendus sont de la forme :

```
access-list <numéro d'ACL> {deny | permit} <protocole> <adresse d'origine> <masque
générique> <adresse destination> <masque générique> <opérateur> <opérande> [established]
```

- **deny** : rejet du paquet
- **permit** : acceptation du paquet

- ✗ **protocole** : détermine le protocole des paquets (icmp, tcp, udp ou ip)
- ✗ **adresse d'origine** et **masque générique** : détermine les adresses IP source concernées par ce contrôle.
- ✗ **adresse destination** et **masque générique** : déterminent les adresses IP destination concernées par ce contrôle.
- ✗ **opérateur et opérande** : permettent de filtrer les paquets selon les ports :
  - ✔ Les opérandes possibles sont :lt (plus petit que), gt (plus grand que), eq (égal à) et neq (différent de).
  - ✔ L'opérande est le numéro de port

Opérande	Alias	Paramètre	Résultat
<	lt	num_port	vrai si le port est inférieur
>	gt	num_port	vrai si le port est supérieur
=	eq	num_port	vrai si le port est égal
!=	ne	num_port	vrai si le port n'est pas égal
<=	le	num_port	vrai si le port est inférieur ou égal
=>	ge	num_port	vrai si le port est supérieur ou égal

- ✗ **established** : permet au trafic TCP de passer si les bits ACK sont activées.

Exemples :

```
Router(config)#access-list 101 permit tcp any host 172.16.0.1 eq www  Tous les paquets à destination de l'adresse IP 172.16.0.1 port 80 (www) sont acceptés. Il s'agit d'un serveur Web.
Router(config)#access-list 101 deny ip any host 172.16.0.1 Tous les autres paquets pour cette même adresse sont refusés.
Router(config)#access-list 101 permit ip 172.171.3.192  0.0.0.63  209.0.0.128  0.0.0.127
Les paquets venant des adresses IP du sous-réseau 172.171.3.192 à destination du sous-réseau 209.0.0.128 sont routés et non filtrés.
Router(config)#access-list 101 permit icmp any any echo-reply   Toutes les réponses de la commande echo (ping) sont acceptées.
Router(config)#access-list 101 permit tcp any any established   Les paquets qui sont envoyés suite à une connexion venant de l'intranet (connexion établie) sont acceptés.
Router(config)#access-list 101 permit tcp any host 172.17.0.2 eq www   Tous les paquets à destination de la machine 172.17.0.2 avec le port source 80 (www) sont acceptés pour toutes les adresses.
Router(config)#access-list 101 permit udp host 172.17.0.2 eq 45 any
Tous les paquets provenant de la machine 172.17.0.2 avec le port source 45 en UDP sont acceptés pour toutes les adresses.
Router(config)#access-list 101 permit udp host 172.17.0.2 eq domain any  Tous les paquets provenant du serveur DNS (172.17.0.2) sont acceptés pour toutes les adresses.
Router(config)#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.
Router(config)#int fa0/0
Router(config-if)#ip access-group 101 in      Application la liste d'accès 101 en entrée sur l'interface fa0/0.
Router(config-if)#exit
```

Le format des ACL étendues par type de protocole est :

IP

access-list *access-list-number*

[dynamic *dynamic-name* **[timeout** *minutes***]]**
{deny|permit} *protocol source source-wildcard*
destination destination-wildcard **[precedence** *precedence***]**
[tos *tos***] [log|log-input] [time-range** *time-range-name***]**

ICMP

access-list *access-list-number*
[dynamic *dynamic-name* **[timeout** *minutes***]]**
{deny|permit} icmp *source source-wildcard*
destination destination-wildcard
[*icmp-type* **[***icmp-code***] |***icmp-message***]**
[precedence *precedence***] [tos** *tos***] [log|log-input]**
[time-range *time-range-name***]**

Le champ icmp-type est le type de message ICMP, il peut être égal à echo-request ou echo-reply.

TCP

access-list *access-list-number*
[dynamic *dynamic-name* **[timeout** *minutes***]]**
{deny|permit} tcp *source source-wildcard* **[operator [***port***]]**
destination destination-wildcard **[operator [***port***]]**
[established] [precedence *precedence***] [tos** *tos***]**
[log|log-input] [time-range *time-range-name***]**

established : indique qu'il s'agit d'une communication TCP déjà établie.

UDP

access-list *access-list-number*
[dynamic *dynamic-name* **[timeout** *minutes***]]**
{deny|permit} udp *source source-wildcard* **[operator [***port***]]**
destination destination-wildcard **[operator [***port***]]**
[precedence *precedence***] [tos** *tos***] [log|log-input]**
[time-range *time-range-name***]**

VIII Les ACL nommées

Les listes de contrôle d'accès nommées IP ont été introduites dans la plate-forme logicielle Cisco IOS version 11.2, afin d'attribuer des noms aux listes d'accès standard et étendues à la place des numéros.

Les commandes pour les ACL étendus sont de la forme :

```
access-list {standard | extended} <nom de l'ACL> <instructions>
```

- ✗ **{standard | extended}** : type d'ACL.
- ✗ **nom de l'ACL** : nom identifiant l'ACL.
- ✗ **instructions** : instructions similaires à access-list en retirant access-list <numéro d'ACL>.

Exemple :

```
Router(config)#ip access-list standard no_access
Router(config-std-nacl)#deny 192.168.14.0   0.0.0.255
Router(config-std-nacl)#permit any
Router(config-std-nacl)#exit
Router(config)#int e0
Router(config-if)#ip access-group no_access in
Router(config-if)#^Z
```