# Recommandations Cisco pour les ACL

Les règles de base suivantes doivent être respectées lors de la création et de l'application des listes d'accès :

- Une liste d'accès par direction et par protocole.
- Les listes d'accès **standard** doivent être appliquées **le plus près possible de la destination**.
- Les listes d'accès **étendues** doivent être appliquées **le plus près possible de la source**.
- Pour faire référence à une interface d'entrée ou de sortie, placez-vous à l'intérieur du routeur en regardant l'interface en question.
- Les instructions sont traitées dans l'ordre depuis le début de la liste jusqu'à la fin jusqu'à ce qu'une correspondance soit trouvée. Si aucune correspondance n'est détectée, le paquet est refusé.
- Il existe un refus implicite **deny any** à la fin de toutes les listes de contrôle d'accès. Cela n'apparaît pas dans la liste de configuration.
- Les entrées de la liste d'accès doivent filtrer les paquets dans l'ordre, du plus spécifique au plus général. Les hôtes spécifiques doivent être rejetés en premier, tandis que les groupes ou les filtres généraux viennent en dernier.
- La condition de correspondance est examinée en premier. L'acceptation ou le refus est examiné UNIQUEMENT si la condition est vraie.
- Ne travaillez jamais avec une liste d'accès qui est appliquée de manière active.
- Utilisez un éditeur de texte pour créer des commentaires indiquant la logique, puis ajoutez les instructions correspondantes.
- Les nouvelles lignes sont toujours ajoutées à la fin de la liste de contrôle d'accès. La commande **no access-list**x supprime toute la liste. Il n'est pas possible d'ajouter et de supprimer des lignes spécifiques dans des listes d'accès numérotées.
- Une liste d'accès IP envoie un message ICMP d'hôte inaccessible à l'émetteur du paquet rejeté et élimine le paquet dans la corbeille prévue à cet effet.
- Soyez particulièrement attentif lorsque vous supprimez une liste d'accès. Si la liste d'accès est appliquée à une interface de production et que vous la supprimez, selon la version de l'IOS, une instruction **deny any** peut être appliquée par défaut à l'interface et tout le trafic peut être arrêté.
- Les filtres de sortie ne concernent pas le trafic généré par le routeur local.

## Exemples d'ACL simples :

access-list <n°> <permit ou deny> host <adr-hôte>
ou <adresse-réseau> <masque-générique>

L'ACL suivante interdit les requêtes provenant de l'hôte 192.168.0.1

```
access-list 10 deny host 192.168.0.1
```

L'ACL suivante interdit les requêtes provenant du réseau 192.168.0.0

```
access-list 10 permit 192.168.0.0 0.0.0.255
```

On applique l'ACL 10 à la sortie de l'interface FastEthernet 0/0

```
interface f0/0
     ip access-group 10 out
```

## Exemples d'ACL étendues :

access-list <n°> permit ou deny
<ip, icmp, tcp, udp>
<ip-source>
<gt | lt | eq> <n°port>
<ip-destination>
<gt | lt | eq> <n°port>

Cette ACL permet aux clients du réseau 192.168.0.0 d'aller visiter le serveur Web :

```
access-list 101 permit tcp 192.168.0.0 0.0.0.255 gt 1023
                                          host  192.168.1.1 eq 80
```

Permettre les requêtes ICMP du réseau 172.16.0.0 au 172.17.0.0

```
access-list 101 permit icmp 172.16.0.0 0.0.0.255 172.17.0.0 0.0.0.255
```

On applique l'ACL 101 à l'entré de l'interface FastEthernet 0/0

```
interface f0/0
     ip access-group 101 in
```

## Exemples d'ACL nommées :

ip access-list extended <nom> permit <ip, icmp, tcp, udp>
<ip-source> <gt,lt,eq> <n°port> <ip-dest> <gt,lt,eq> <n°port>

L'ACL suivante permet aux clients du réseau 192.168.0.0/24 d'aller visiter le serveur Web et DNS :

```
ip access-list extended monacl
      permit tcp 192.168.0.0 0.0.0.255 gt 1023 host 192.168.1.1 eq 80
      permit udp 192.168.0.0 0.0.0.255 gt 1023 host 192.168.2.1 eq 53
```

On applique l'ACL **monacl** à l'entré de l'interface FastEthernet 0/0

```
interface f0/0
      ip access-group monacl in
```