

SIO SISR sur

# ACL sous Cisco IOS

Apprendre à configurer et à appliquer des ACL sur les équipements  
CISCO

## Table des matières

Introduction : Listes de Contrôle d'Accès (ACL) sur les Équipements CISCO .....	3
Contexte.....	3
Définition d'une ACL.....	3
Importance des ACL.....	3
Comment fonctionnent les ACL sur les Équipements CISCO.....	3
1. Concepts fondamentaux des ACL.....	4
1.1 Qu'est-ce qu'une ACL ?.....	4
Définition : .....	4
Fonctionnement : .....	4
Applications courantes : .....	4
1.2 Types d'ACL : .....	4
ACL standard :.....	4
ACL étendue : .....	4
ACL nommée : .....	5
1.3 L'ordre des règles : .....	5
1.4 Action implicite "Deny All" : .....	5
1.5 Bonnes pratiques : .....	5
2. Configuration des ACL sur les équipements CISCO .....	5
2.1 Configuration d'une ACL standard : .....	5
2.2 Configuration d'une ACL étendue : .....	6
2.3 Configuration d'une ACL nommée : .....	6
2.4 Application des ACL aux interfaces : .....	7
2.5 Bonnes pratiques lors de la configuration des ACL : .....	7
3. Application des ACL .....	8
3.1 Direction des ACL : .....	8
3.2 Application à une interface : .....	8
3.3 Vérification de l'application : .....	8
3.4 Retrait ou Modification d'une ACL appliquée : .....	9
4. Bonnes pratiques pour les ACL .....	9
4.1 Priorisation des règles : .....	9
4.2 Expliciter l'implémentation : .....	9
4.3 Documentation : .....	9
4.4 Testez avant de déployer : .....	10
4.5 Revue régulière : .....	10
4.6 Limitez la taille des ACL : .....	10

4.7 Sauvegardez régulièrement :	10
5. Dépannage des ACL	10
5.1 Vérification de la configuration :	10
5.2 Testez le trafic :	11
5.3 Comprendre les comportements par défaut :	11
5.4 Modifiez et testez de manière incrémentielle :	11
5.5 Vérifiez les journaux :	11
5.6 Considérez d'autres facteurs :	11

# Introduction : Listes de Contrôle d'Accès (ACL) sur les Équipements CISCO

## Contexte

Dans le monde numérique actuel, la gestion du trafic réseau est devenue un élément essentiel pour assurer la sécurité, l'efficacité et la performance d'un réseau. Les entreprises, grandes et petites, ont besoin de méthodes robustes pour contrôler quel trafic est autorisé à entrer, sortir ou traverser leur réseau. C'est ici que les ACL (Access Control Lists) entrent en jeu.

## Définition d'une ACL

Une ACL est fondamentalement une série de règles que vous appliquez à un point d'entrée ou de sortie d'un périphérique, comme une interface sur un routeur ou un commutateur. Chaque règle spécifie un ensemble de conditions que le trafic doit remplir pour être autorisé ou refusé. Si le trafic correspond à une condition, une action associée (généralement "permit" ou "deny") est exécutée.

## Importance des ACL

1. **Sécurité** : Les ACL peuvent empêcher des utilisateurs non autorisés d'accéder à certaines parties du réseau. Par exemple, un administrateur pourrait utiliser une ACL pour empêcher le trafic provenant d'une adresse IP suspecte.
2. **Gestion du Trafic** : Les ACL permettent de garantir que le trafic de haute priorité obtienne la bande passante nécessaire, ou que certains types de trafic soient redirigés vers des chemins spécifiques.
3. **Politiques d'entreprise** : Les ACL aident à appliquer des politiques d'entreprise, comme l'interdiction de l'accès à des sites de réseaux sociaux pendant les heures de travail.

## Comment fonctionnent les ACL sur les Équipements CISCO

Sur les équipements CISCO, les ACL sont traitées en séquence. Lorsque le trafic arrive à une interface où une ACL est appliquée, le périphérique examine chaque entrée de l'ACL dans l'ordre, de haut en bas. Lorsqu'il trouve une correspondance, il exécute l'action associée et arrête de vérifier les autres entrées. Si aucune correspondance n'est trouvée après avoir vérifié toutes les entrées, le trafic est refusé par défaut. Cette action "deny all" implicite à la fin de chaque ACL est un élément crucial à comprendre.

# 1. Concepts fondamentaux des ACL

## 1.1 Qu'est-ce qu'une ACL ?

### Définition :

Une Liste de Contrôle d'Accès (ACL) est une liste séquentielle de règles utilisées pour filtrer le trafic. Chaque règle définit un ensemble de conditions que les paquets doivent satisfaire. Si un paquet remplit ces conditions, une action prédéfinie (généralement "permit" ou "deny") est prise.

### Fonctionnement :

Les ACLs traitent les paquets un par un, en vérifiant chaque paquet par rapport à la liste de règles, de haut en bas. Lorsqu'une correspondance est trouvée, l'action associée est prise et le traitement des règles suivantes s'arrête. Si aucun critère n'est satisfait, l'action par défaut est "deny".

### Applications courantes :

- Filtrage du trafic.
- Redirection du trafic pour la surveillance ou la capture.
- Gestion de la bande passante.
- Sécurisation de l'accès au réseau ou à des ressources spécifiques.

## 1.2 Types d'ACL :

### ACL standard :

- Ces ACL filtrent uniquement sur la base des adresses IP source.
- La plage de numéros pour les ACL standard est généralement de 1 à 99 et de 1300 à 1999 pour les ACL nommées.
- Exemple : `access-list 10 deny 192.168.1.0 0.0.0.255``

### ACL étendue :

- Ces ACL filtrent sur la base des adresses IP source et de destination, des protocoles, des ports et d'autres critères.
- La plage de numéros pour les ACL étendues est généralement de 100 à 199 et de 2000 à 2699 pour les ACL nommées.
- Exemple : `access-list 101 deny tcp 192.168.1.0 0.0.0.255 any eq www``

ACL nommée :

- Ces ACL permettent d'utiliser des noms descriptifs au lieu de numéros, offrant une meilleure documentation.
- Peuvent être standard ou étendues.
- Exemple : ``ip access-list extended Block-Web-Traffic``

### 1.3 L'ordre des règles :

La manière dont les règles sont ordonnées dans une ACL est cruciale. Étant donné que le traitement s'arrête dès qu'une correspondance est trouvée, si une règle large (comme ``permit ip any any``) est placée au début, les règles suivantes ne seront jamais évaluées. Il est donc essentiel de placer les règles les plus spécifiques en haut et les règles plus générales en bas.

### 1.4 Action implicite "Deny All" :

Chaque ACL, qu'elle soit standard, étendue ou nommée, a une action implicite "deny any" à la fin. Cela signifie que si un paquet ne correspond à aucune des règles spécifiées, il sera refusé. Les administrateurs réseau doivent être conscients de cette action implicite lors de la création d'ACL.

### 1.5 Bonnes pratiques :

- Toujours inclure une règle "permit" explicite à la fin de chaque ACL pour permettre le trafic légitime.
- Testez les ACL dans un environnement contrôlé avant de les déployer.
- Documentez soigneusement chaque règle pour faciliter la maintenance et le dépannage futurs.

## 2. Configuration des ACL sur les équipements CISCO

### 2.1 Configuration d'une ACL standard :

**Définition** : Les ACL standard offrent un filtrage basé uniquement sur l'adresse IP source du paquet.

**Syntaxe** :

```
access-list [numéro] permit|deny [adresse-source] [wildcard-mask]
```

**Exemple** : Pour bloquer tout le trafic provenant du réseau 192.168.1.0/24:

```
access-list 10 deny 192.168.1.0 0.0.0.255
```

```
access-list 10 permit any
```

## 2.2 Configuration d'une ACL étendue :

**Définition** : Les ACL étendues offrent un filtrage basé sur l'adresse IP source, l'adresse IP de destination, le protocole, le port et d'autres critères.

**Syntaxe** :

```
access-list [numéro] permit|deny [protocole] [adresse-source] [wildcard-mask] [adresse-destination] [wildcard-mask] [conditions optionnelles]
```

**Exemple** : Pour bloquer le trafic HTTP (port 80) de 192.168.1.0/24 vers n'importe quelle destination :

```
access-list 110 deny tcp 192.168.1.0 0.0.0.255 any eq 80
access-list 110 permit ip any any
```

## 2.3 Configuration d'une ACL nommée :

**Définition** : Les ACL nommées offrent la même fonctionnalité que les ACL numérotées mais utilisent des noms descriptifs pour une meilleure documentation.

**Syntaxe pour ACL standard nommée** :

```
ip access-list standard [nom-acl]
    permit|deny [adresse-source] [wildcard-mask]
```

**Syntaxe pour ACL étendue nommée** :

```
ip access-list extended [nom-acl]
    permit|deny [protocole] [adresse-source] [wildcard-mask] [adresse-destination] [wildcard-mask] [conditions optionnelles]
```

**Exemple pour ACL étendue nommée** : Pour bloquer le trafic SSH (port 22) de 192.168.2.0/24 vers n'importe quelle destination:

```
ip access-list extended Block-SSH
    deny tcp 192.168.2.0 0.0.0.255 any eq 22
    permit ip any any
```

## 2.4 Application des ACL aux interfaces :

Une fois l'ACL créée, elle doit être appliquée à une interface pour prendre effet. L'ACL peut être appliquée dans la direction entrante (in) ou sortante (out) d'une interface.

### Syntaxe :

```
interface [type numéro]
ip access-group [numéro-acl|nom-acl] in|out
```

**Exemple :** Pour appliquer l'ACL précédemment créée (Block-SSH) à l'interface GigabitEthernet0/0 dans la direction entrante :

```
interface GigabitEthernet0/0
ip access-group Block-SSH in
```

## 2.5 Bonnes pratiques lors de la configuration des ACL :

**Séquence des règles :** Gardez à l'esprit l'ordre des règles, les règles les plus spécifiques doivent généralement être placées en haut.

**Validation :** Avant d'appliquer une ACL à une interface, utilisez la commande `show access-list` pour valider la séquence.

**Documentation :** Utilisez des commentaires (`remark`) pour documenter l'intention derrière chaque règle. Par exemple :

```
access-list 110 remark Block HTTP traffic from subnet 192.168.1.0/24
```

**En conclusion,** la configuration des ACL sur les équipements CISCO offre une flexibilité et un contrôle granulaires pour le filtrage du trafic. Une compréhension claire de la syntaxe et des bonnes pratiques garantira une mise en œuvre efficace et sécurisée des politiques de réseau.



## 3. Application des ACL

Lorsque vous avez créé une ACL, son efficacité dépend entièrement de la manière dont elle est appliquée. La mise en application d'une ACL est le processus d'association de cette liste à une interface réseau, déterminant ainsi comment et où le trafic est filtré.

### 3.1 Direction des ACL :

#### **Entrant ('in') :**

Lorsqu'une ACL est appliquée à une interface dans la direction entrante, elle évalue le trafic avant qu'il ne soit routé à travers le périphérique. Par exemple, si une ACL est appliquée à l'interface entrante d'un routeur, elle filtrera les paquets juste après leur réception sur cette interface, avant que le routeur ne prenne une décision de routage.

#### **Sortant ('out') :**

Inversement, une ACL configurée pour une direction sortante filtrera le trafic après que le périphérique ait pris sa décision de routage. Les paquets sont évalués juste avant de quitter l'interface.

### 3.2 Application à une interface :

Après avoir défini une ACL, vous devez l'appliquer à une interface pour qu'elle affecte le trafic. La syntaxe générale est :

```
interface [type numéro]
ip access-group [numéro-acl|nom-acl] in|out
```

Par exemple, pour appliquer une ACL nommée "Block-SSH" à l'interface GigabitEthernet0/0 dans la direction entrante :

```
interface GigabitEthernet0/0
ip access-group Block-SSH in
```

### 3.3 Vérification de l'application :

Une fois que vous avez appliqué une ACL, il est essentiel de vérifier son fonctionnement. Vous pouvez le faire en utilisant des commandes telles que :

- ``show access-lists`` : affiche les ACL et leurs compteurs de correspondance.
- ``show ip interface`` : pour voir les ACL appliquées à chaque interface.

### 3.4 Retrait ou Modification d'une ACL appliquée :

Si vous devez modifier une ACL déjà appliquée, il est généralement recommandé de retirer l'ACL de l'interface, de faire vos modifications, puis de réappliquer l'ACL. Cela permet de prévenir tout comportement inattendu du trafic pendant le processus de modification.

**En résumé**, l'application correcte des ACL est cruciale pour garantir qu'elles fonctionnent comme prévu. Une fois définies, ces listes doivent être associées à des interfaces et à des directions spécifiques pour filtrer le trafic entrant ou sortant. Une surveillance et une vérification régulières garantiront que votre réseau fonctionne de manière optimale et sécurisée.

## 4. Bonnes pratiques pour les ACL

La mise en œuvre efficace des ACL nécessite non seulement une compréhension technique, mais aussi une approche stratégique pour éviter des erreurs courantes. Voici les bonnes pratiques clés pour utiliser les ACL sur les équipements Cisco.

### 4.1 Priorisation des règles :

L'ordre dans lequel les règles sont énoncées dans une ACL est crucial. Les paquets sont évalués selon ces règles de haut en bas. Ainsi, les règles les plus spécifiques doivent être placées avant les règles plus générales pour éviter des correspondances non intentionnelles. Si une règle générale est placée en premier, elle peut potentiellement "éclipser" toutes les règles qui suivent.

### 4.2 Expliciter l'implémentation :

Même si toutes les ACL ont une règle implicite "deny any" à la fin, il est considéré comme une bonne pratique d'ajouter explicitement cette règle à la fin de vos ACL. Cela rend la liste plus lisible et évite toute confusion.

### 4.3 Documentation :

Il est essentiel de documenter chaque ACL et chaque règle au sein de cette ACL. Utilisez la commande ``remark`` pour ajouter des commentaires décrivant le but ou la raison d'une règle particulière. Cette documentation facilite la maintenance et le dépannage à long terme.

#### 4.4 Testez avant de déployer :

Avant d'appliquer une nouvelle ACL ou de modifier une ACL existante, testez-la d'abord dans un environnement contrôlé. Cela permet de s'assurer qu'elle fonctionne comme prévu sans interrompre le trafic légitime.

#### 4.5 Revue régulière :

Avec le temps, les besoins du réseau peuvent changer. Il est bon de revoir et d'auditer régulièrement les ACL pour s'assurer qu'elles sont toujours pertinentes et ne contiennent pas de règles obsolètes.

#### 4.6 Limitez la taille des ACL :

Des ACL trop longues peuvent affecter les performances de l'équipement et rendre la gestion plus complexe. Essayez de garder vos ACL aussi concises que possible tout en répondant aux besoins du réseau.

#### 4.7 Sauvegardez régulièrement :

Assurez-vous de sauvegarder régulièrement la configuration de votre équipement, notamment après avoir apporté des modifications aux ACL. Cela garantit que vous pouvez rapidement restaurer la configuration en cas de problème.

### 5. Dépannage des ACL

La mise en place d'ACL est une tâche délicate. Même avec une planification minutieuse, il peut y avoir des problèmes. Dans cette section, nous allons aborder les étapes et outils essentiels pour le dépannage des ACL.

#### 5.1 Vérification de la configuration :

La première étape pour résoudre tout problème lié aux ACL est de vérifier si la configuration est correcte.

- Utilisez la commande ``show access-list`` pour voir les ACL configurées et leurs compteurs de correspondance.
- Assurez-vous que l'ordre des règles est logique. Rappelez-vous, les paquets sont évalués en fonction de l'ordre de haut en bas des règles d'une ACL.
- Avec la commande ``show ip interface``, vous pouvez déterminer si une ACL est correctement appliquée à une interface et dans la bonne direction (entrante ou sortante).

## 5.2 Testez le trafic :

Après avoir vérifié la configuration, testez le trafic pour vous assurer qu'il est traité comme prévu.

- Vous pouvez utiliser des outils comme ``ping`` ou des utilitaires de test de port pour vérifier si un trafic spécifique est autorisé ou bloqué.
- La commande ``debug ip packet detail`` peut également être utilisée pour suivre les paquets traités par un routeur. Toutefois, faites preuve de prudence avec les commandes de débogage, car elles peuvent surcharger l'équipement.

## 5.3 Comprendre les comportements par défaut :

Rappelez-vous que chaque ACL a une règle implicite "deny any" à la fin, même si elle n'est pas affichée. Si un paquet ne correspond à aucune règle spécifiée, il sera refusé. Cela peut souvent être la cause d'un trafic inattendu étant bloqué.

## 5.4 Modifiez et testez de manière incrémentielle :

Lorsque vous apportez des modifications à une ACL pour résoudre des problèmes, faites-le par étapes. Après chaque modification, testez pour voir si le problème est résolu. Cela vous permet d'isoler rapidement la source du problème.

## 5.5 Vérifiez les journaux :

Les équipements Cisco peuvent enregistrer des informations sur le trafic qui est autorisé ou refusé par une ACL.

- Utilisez la commande ``show logging`` pour afficher les journaux.
- Si vous ne voyez pas les entrées pertinentes, assurez-vous que le niveau de journalisation est configuré correctement.

## 5.6 Considérez d'autres facteurs :

Parfois, un problème peut sembler être lié à une ACL, mais la cause peut être ailleurs. Par exemple, des problèmes de connectivité réseau, de configuration IP ou de routage peuvent également entraîner des symptômes similaires à ceux d'une ACL mal configurée.

**En résumé**, le dépannage des ACL nécessite une approche méthodique. Les outils de débogage et de journalisation fournis par Cisco sont essentiels pour comprendre et résoudre rapidement les problèmes. Une fois que vous avez acquis une expérience dans le dépannage des ACL, vous serez mieux équipé pour gérer et sécuriser efficacement votre réseau.

## 6. Atelier pratique : Configuration et dépannage des ACL sur Cisco

L'atelier pratique vise à offrir une expérience concrète et à renforcer la compréhension des ACL. Dans cet atelier, nous configurerons, appliquerons, et dépannerons des ACL sur un équipement Cisco.

### **Objectif :**

Configurer une ACL pour restreindre l'accès SSH à un routeur Cisco uniquement depuis un réseau spécifique.

### **Matériel nécessaire :**

- Routeur Cisco avec au moins deux interfaces.
- Deux PC ou simulateurs de PC.
- Câbles Ethernet pour la connexion.

### **Scénario :**

Un PC (PC1) se trouve dans le réseau autorisé (192.168.1.0/24) et l'autre PC (PC2) dans un réseau non autorisé (192.168.2.0/24). Seul PC1 devrait pouvoir accéder au routeur via SSH.

### 6.1 Configuration initiale :

1. Assurez-vous que le routeur est configuré avec SSH activé.
2. Configurez les interfaces du routeur avec les adresses IP appropriées.
3. Assurez-vous que les deux PC ont des configurations IP correspondantes et peuvent atteindre le routeur.

### 6.2 Création de l'ACL :

Sur le routeur, entrez le mode de configuration :

```
Router> enable
```

```
Router# configure terminal
```

Créez une ACL nommée "SSH-ACCESS" :

```
Router(config)# ip access-list extended SSH-ACCESS
```

Autorisez le trafic SSH depuis le réseau 192.168.1.0/24 :

```
Router(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any eq 22
```

Bloquez tout autre trafic SSH :

```
Router(config-ext-nacl)# deny tcp any any eq 22
```

### 6.3 Appliquer l'ACL :

Appliquez l'ACL à l'interface appropriée dans la direction entrante :

```
Router(config)# interface GigabitEthernet0/0
```

```
Router(config-if)# ip access-group SSH-ACCESS in
```

### 6.4 Testez la configuration :

1. Depuis PC1, tentez une connexion SSH au routeur. Elle devrait réussir.
2. Depuis PC2, tentez une connexion SSH au routeur. Elle devrait échouer.

### 6.5 Dépannage :

Si les tests ne donnent pas les résultats escomptés :

- Vérifiez la configuration IP des PC et du routeur.
- Utilisez la commande `show access-lists` pour voir si les paquets correspondent à l'ACL.
- Assurez-vous que l'ACL est correctement appliquée à l'interface et dans la bonne direction.

## Conclusion

Les listes de contrôle d'accès (ACL) sont essentielles pour gérer et sécuriser les réseaux, offrant aux administrateurs réseau un moyen précis de contrôler le trafic à travers les équipements, notamment ceux de Cisco. Cette formation a couvert l'éventail des ACL, de la théorie à la pratique, soulignant leur importance dans un monde axé sur la sécurité. Une mise en œuvre adéquate des ACL

garantit un accès approprié aux ressources, tout en bloquant le trafic indésirable. Toutefois, une mauvaise gestion peut entraîner des perturbations. Par la formation et la pratique régulière, on peut non seulement maîtriser les ACL, mais aussi s'adapter aux évolutions du paysage technologique.