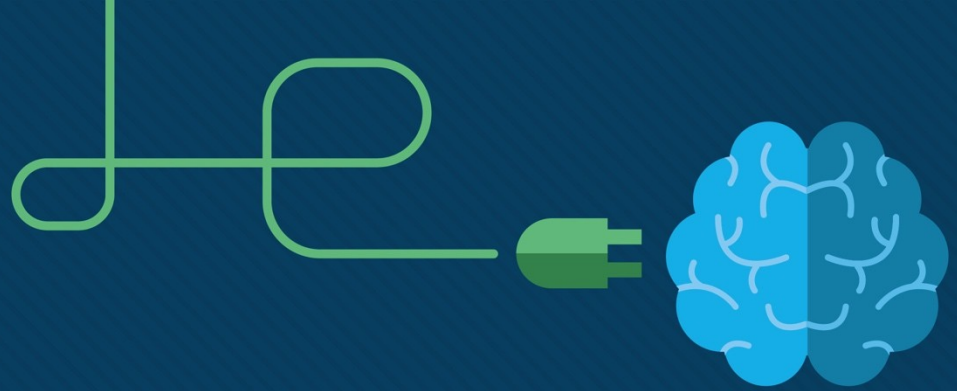


# Module : Concepts ACL

Réseau, Sécurité et Automatisation D'entreprise v7.0 (ENSA)

# Objectifs de ce module

**Titre du module:** Concepts ACL

**Objectif du module**: Expliquer comment les listes de contrôle d'accès sont utilisées dans le cadre d'une politique de sécurité réseau.

| Titre du rubrique | Objectif du rubrique |
|---|---|
| **Objectif des listes de contrôle d'accès** | Expliquer comment les listes de contrôle d'accès filtrent le trafic |
| **Masques génériques dans les listes de contrôle d'accès** | Expliquer comment les listes de contrôle d'accès utilisent des masques génériques. |
| **Création de listes de contrôle d'accès** | Expliquer comment créer des listes de contrôle d'accès. |
| **Types de listes de contrôle d'accès IPv4** | Comparer les listes de contrôle d'accès IPv4 standard et étendues. |

# .1 Objectif des listes de contrôle d'accès (ACL)

# Qu'est-ce qu'une liste de contrôle d'accès?

Une liste de contrôle d'accès (ou ACL) est une série de commandes IOS qui déterminent si un routeur achemine ou abandonne les paquets en fonction des informations contenues dans l'en-tête de paquet. Par défaut, aucun ACL n'est configuré pour un routeur. Toutefois, lorsqu'une liste de contrôle d'accès est appliquée à une interface, le routeur évalue en outre tous les paquets réseau lorsqu'ils traversent l'interface pour déterminer s'ils peuvent être acheminés.

- Une ACL utilise une liste séquentielle de déclarations d'autorisation ou de refus, connues sous le nom d'entrées de contrôle d'accès (ACE).

**Remarque:** Les ACE sont couramment appelées des instructions de liste de contrôle d'accès.

- Lorsque le trafic réseau traverse une interface configurée avec une liste de contrôle d'accès, le routeur compare les informations du paquet à chaque ACE, dans l'ordre séquentiel, afin de déterminer si le paquet correspond à l'une des entrées ACE. C’est ce que l’on appelle le filtrage de paquet.

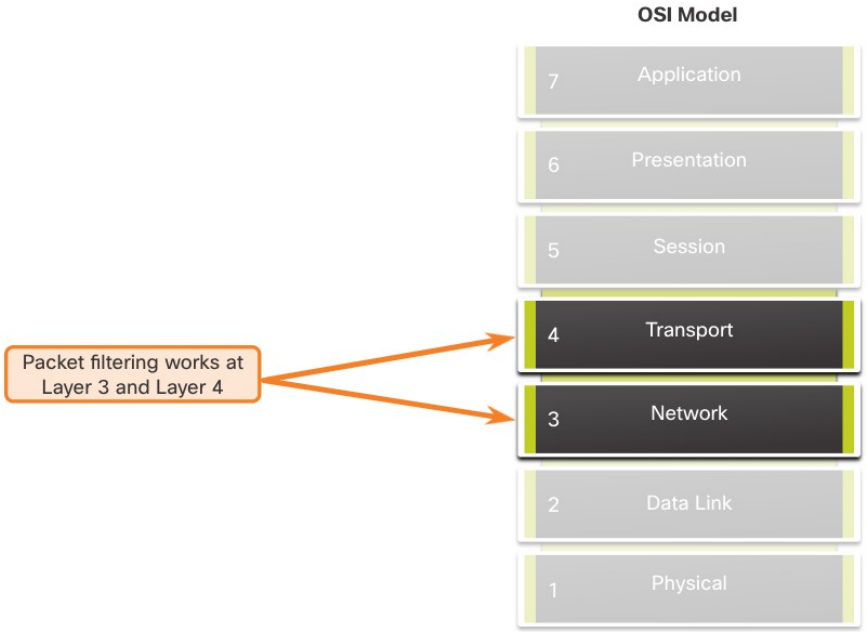
# Qu'est-ce qu'une liste de contrôle d'accès? (Suite)

Plusieurs tâches effectuées par les routeurs nécessitent l'utilisation d'ACL pour identifier le trafic:

- Limiter le trafic du réseau pour en augmenter les performances
- Elles contrôlent le flux de trafic.
- Elles fournissent un niveau de sécurité de base pour l'accès réseau.
- Elles filtrent le trafic en fonction de son type.
- Contrôler les hôtes pour autoriser ou refuser l'accès aux services de réseau
- Donner la priorité à certaines classes de trafic réseau

# Filtrage des paquets

- Le filtrage de paquets contrôle l'accès à un réseau en analysant les paquets entrants et/ou sortants et en les transmettant ou en les abandonnant en fonction de critères donnés.
- Le filtrage des paquets peut être effectué au niveau de la couche 3 ou de la couche 4.
- Les routeurs Cisco prennent en charge deux types de ACLs:
  - **ACL standard** - Les ACL filtrent uniquement au niveau de la couche 3 à l'aide de l'adresse IPv4 source uniquement.
  - **ACL étendues** - Filtre ACL à la couche 3 à l'aide de l'adresse IPv4 source et/ou destination. Ils peuvent également filtrer au niveau de la couche 4 en utilisant les ports TCP et UDP, ainsi que des informations facultatives



# Le fonctionnement des listes de contrôle d'accès

- Les listes de contrôle d'accès définissent des règles de contrôle pour les paquets arrivant par les interfaces d'entrée, passant par le routeur et atteignant leur destination par les interfaces de sortie.
- Les listes de contrôle d'accès peuvent être configurées pour s'appliquer au trafic entrant et au trafic sortant:

**Remarque**: Les ACL ne gèrent pas les paquets provenant du routeur lui-même.

- Un ACL entrant filtre les paquets avant qu'ils ne soient acheminés vers l'interface sortante. Une liste de contrôle d’accès entrante est efficace car elle réduit la charge des recherches de routage en cas d’abandon du paquet.
- Les listes de contrôle d'accès sortantes filtrent les paquets après qu'ils ont été routés, et ce, quelle que soit l'interface de sortie.

# Le fonctionnement des listes de contrôle d'accès (Suite)

Lorsqu'une ACL est appliquée à une interface, elle suit une procédure d'exploitation spécifique. Voici les étapes opérationnelles utilisées lorsque le trafic est entré dans une interface de routeur avec une ACL IPv4 standard entrante configurée:

1. Le routeur extrait l'adresse IPv4 source de l'en-tête du paquet.
2. Le routeur commence en haut de l'ACL et compare l'adresse IPv4 source à chaque ACE dans un ordre séquentiel.
3. Lorsqu'une correspondance est établie, le routeur exécute l'instruction, soit en autorisant soit en refusant le paquet, et les ACE restants dans l'ACL, le cas échéant, ne sont pas analysés.
4. Si l'adresse IPv4 source ne correspond à aucun ACE de l'ACL, le paquet est ignoré car un ACE de refus implicite est automatiquement appliqué à toutes les ACLs.

La dernière instruction d'une liste de contrôle d'accès est toujours une instruction deny implicite bloquant tout le trafic. Il est caché et non affiché dans la configuration.

**Remarque**: Une liste ACL doit avoir au moins une déclaration d'autorisation sinon tout le trafic sera refusé en raison de l'instruction ACE de refus implicite.

# .2 - Masques génériques dans les listes de contrôle d'accès

# Présentation de masques génériques

Un masque générique est similaire à un masque de sous-réseau en ce sens qu'il utilise le processus AnDing pour identifier les bits d'une adresse IPv4 à correspondre. En effet, contrairement à un masque de sous-réseau, où le chiffre binaire 1 équivaut à une correspondance et le chiffre binaire 0 à une non-correspondance, les masques génériques procèdent de façon inverse.

- Un ACE IPv4 utilise un masque générique 32 bits pour déterminer quels bits de l'adresse à examiner pour rechercher une correspondance.
- Les masques génériques respectent les règles suivantes pour faire correspondre les chiffres binaires 1 et 0:
  - **Bit 0 de masque générique** - permet de vérifier la valeur du bit correspondant dans l'adresse.
  - **Masque générique bit 1** - Ignorer la valeur du bit correspondant dans l'adresse

# Présentation de masques génériques (Suite)

| Masque générique | Dernier octet (en binaire) | Signification (0 - match, 1 - ignorer) |
|---|---|---|
| **0.0.0.0** | **00000000** | Correspond à tous les octets. |
| **0.0.0.63** | **00111111** | •Faites correspondre les trois premiers octets<br>•Correspond aux deux bits les plus à gauche du dernier octet<br>•Les 6 derniers bits d'adresse sont ignorés |
| **0.0.0.15** | **00001111** | •Faites correspondre les trois premiers octets<br>•Correspond aux quatre bits les plus à gauche du dernier octet<br>•Ignorer les 4 derniers bits du dernier octet |
| **0.0.0.248** | **11111100** | •Faites correspondre les trois premiers octets<br>•Ignorer les six bits les plus à gauche du dernier octet<br>•Faites correspondre les deux derniers bits |
| **0.0.0.255** | **11111111** | •Faites correspondre les trois premiers octet<br>•Ignorer le dernier octet |

# Types de masques génériques

**Caractère générique pour correspondre à un hôte:**

- Supposons que l'ACL 10 ait besoin d'un ACE qui autorise uniquement l'hôte avec l'adresse IPv4 192.168.1.1. Rappelez-vous que "0" équivaut à une correspondance et "1" à une ignorance. Pour correspondre à une adresse IPv4 d'hôte spécifique, un masque générique composé de tous les zéros (c.-à-d. 0.0.0.0) est requis.
- Lorsque l'ACE est traité, le masque générique n'autorisera que l'adresse 192.168.1.1. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.1.1 0.0.0.0.**

| | Décimal | Binaire |
|---|---|---|
| Adresse IPv4 | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Masque générique | 0.0.0.0 | 00000000.00000000.00000000.00000000 |
| **Adresse IPv4 autorisée** | **192.168.1.1** | **11000000.10101000.00000001.00000001** |

# Types de masques génériques (Suite)

**Masques génériques correspondant à des sous-réseaux IPv4**

- ACL 10 a besoin d'un ACE qui autorise tous les hôtes du réseau 192.168.1.0/24. Le masque générique 0.0.0.255 stipule que les trois premiers octets doivent correspondre exactement, mais pas le quatrième octet.
- Lorsqu'il est traité, le masque générique 0.0.0.255 autorise tous les hôtes du réseau 192.168.1.0/24. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.1.0 0.0.0.255.**

| | Décimal | Binaire |
|---|---|---|
| Adresse IPv4 | 192.168.1.1 | 11000000.10101000.00000001.00000001 |
| Masque générique | 0.0.0.255 | 00000000.00000000.00000000.11111111 |
| **Adresse IPv4 autorisée** | **192.168.1.0/24** | 11000000.10101000.00000001.00000000 |

# Types de masques génériques (Suite)

**Masque générique pour correspondre à une plage d'adresses IPv4**

- ACL 10 a besoin d'un ACE qui autorise tous les hôtes des réseaux 192.168.16.0/24, 192.168.17.0/24,..., 192.168.31.0/24.
- Lorsqu'il est traité, le masque générique 0.0.15.255 autorise tous les hôtes des réseaux 192.168.16.0/24 à 192.168.31.0/24. L'ACE résultant dans l'ACL 10 serait **access-list 10 permit 192.168.16.0 0.0.15.255.**

| | Décimal | Binaire |
|---|---|---|
| Adresse IPv4 | 192.168.16.0 | 11000000.10101000.00010000.00000000 |
| Masque générique | 0.0.15.255 | 00000000.00000000.00001111.11111111 |
| **Adresse IPv4 autorisée** | **192.168.16.0/24 à 192.168.31.0/24** | **11000000.10101000.00010000.00000000 à 11000000.10101000.00011111.00000000** |

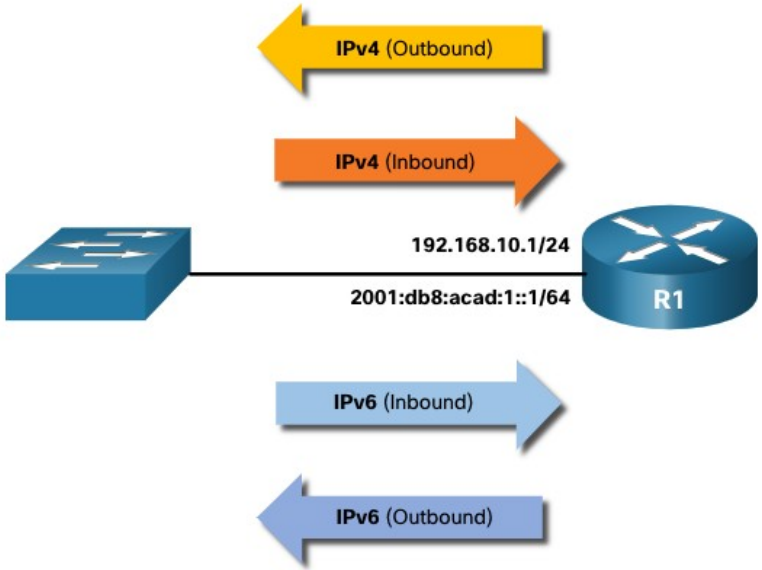
# .3 Directives pour la création de LCA

# Nombre limité d'ACL par interface

Le nombre de listes ACL pouvant être appliquées sur une interface de routeur est limité. Par exemple, une interface de routeur double empilée (c'est-à-dire IPv4 et IPv6) peut avoir jusqu'à quatre ACL appliquées, comme indiqué sur la figure.

Plus précisément, une interface de routeur peut avoir:

- Une liste ACL sortante IPv4.
- Une ACL IPv4 entrante.
- Une ACL IPv6 entrante.
- Une liste ACL IPv6 sortante.




**Remarque**: il n'est pas nécessaire de configurer les listes de contrôle d'accès dans les deux directions. Le nombre d'ACL et leur direction appliquée à l'interface dépendront de la stratégie de sécurité de l'organisation.

# Meilleure pratiques relatives aux listes de contrôle d'accès

L'utilisation des listes de contrôle d'accès nécessite beaucoup de précision et de soin. Les erreurs peuvent vous coûter cher et se solder par des pannes de réseau, d'importants efforts de dépannage et des services réseau médiocres. Une planification de base est nécessaire avant de configurer une ACL.

| Directive | Avantage |
|---|---|
| Créez vos listes de contrôle d'accès conformément à la stratégie de sécurité de votre entreprise. | Vous serez ainsi certain d'implémenter les instructions relatives à la sécurité organisationnelle. |
| Écrivez ce que vous voulez que l'ACL fasse. | Vous éviterez ainsi de créer d'éventuels problèmes d'accès par mégarde. |
| Utilisez un éditeur de texte pour créer, modifier et enregistrer les listes de contrôle d'accès. | Vous pourrez ainsi créer une bibliothèque de listes de contrôle d'accès réutilisables. |
| Documentez les ACL à l'aide de la commande **remark** . | Cela vous aidera (et d'autres) à comprendre le but d'un ACE. |
| Testez vos listes de contrôle d'accès sur un réseau de développement avant de les implémenter sur un réseau de production. | Vous éviterez ainsi de commettre des erreurs coûteuses. |

# .4 Types d'ACL IPv4

# Listes de contrôle d'accès standard et étendues

Types de listes de contrôle d'accès IPv4

- **ACL standard** - Ces listes autorisent ou refusent les paquets basés uniquement sur l'adresse IPv4 source.
- **ACL étendues** - Ces listes autorisent ou refusent les paquets basés sur l'adresse IPv4 source et l'adresse IPv4 de destination, le type de protocole, les ports TCP ou UDP source et destination et plus encore.

# Listes de contrôle d'accès numérotées et nommées

## Listes de contrôle d’accès numérotées

- Les ACL numérotées 1-99 ou 1300-1999 sont des ACL standard, tandis que les ACL numérotées 100-199 ou 2000-2699 sont des ACL étendues.

```
R1(config)# access-list ?
 <1-99> IP standard access list
 <100-199> IP extended access list
 <700-799> 48-bit MAC address access list
 <1300-1999> IP standard access list (expanded range)
 <200-299> Protocol type-code access list
 <2000-2699> IP extended access list (expanded range)
 <700-799> 48-bit MAC address access list
 rate-limit Simple rate-limit specific access list
 template Enable IP template acls
Router(config)# access-list
```

# Listes de contrôle d'accès numérotées et nommées (Suite)

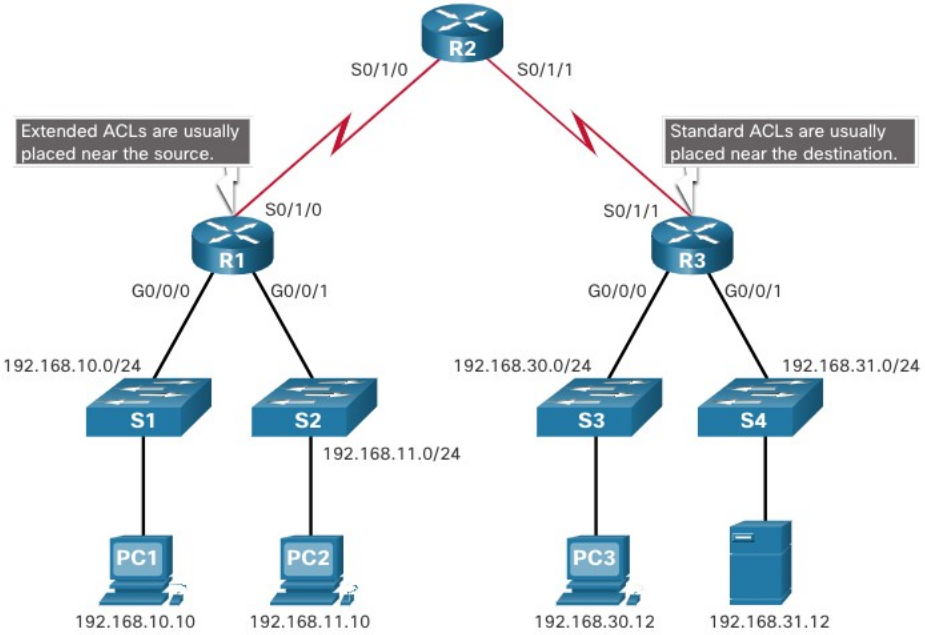
## Listes de contrôle d'accès nommées

- Les ACL nommées sont la méthode préférée à utiliser lors de la configuration des ACL. Plus précisément, les listes ACL standard et étendues peuvent être nommées pour fournir des informations sur l'objet de la liste ACL. Par exemple, nommer un ACL FTP-FILTER étendu est beaucoup mieux que d'avoir une ACL numérotée 100.
- La commande de configuration globale **ip access-list** est utilisée pour créer une liste ACL nommée, comme illustré dans l'exemple suivant.

```
R1(config)# ip access-list extended FTP-FILTER
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp
R1(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 any eq ftp-data
R1(config-ext-nacl)#
```

# Où placer les listes de contrôle d'accès

- Chaque liste de contrôle d'accès doit être placée là où elle aura le plus grand impact sur les performances.
- Les listes de contrôle d'accès étendues doivent être placées le plus près possible de la source du trafic à filtrer.
- Les listes de contrôle d'accès standard doivent être placées le plus près possible de la destination.



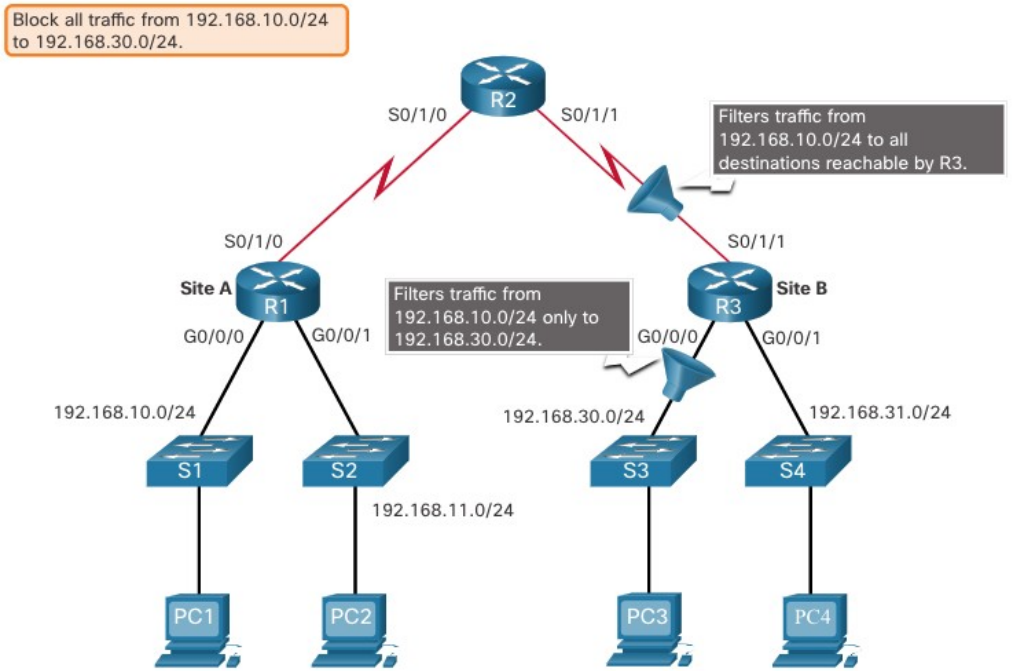
# Où placer les listes de contrôle d'accès (Suite)

| Facteurs influençant le placement des ACL | Explication |
|---|---|
| **L'étendue du contrôle organisationnel** | Le placement de l'ACL peut dépendre du fait que l'organisation contrôle ou non les réseaux source et destination. |
| **Bande passante des réseaux concernés** | Il peut être souhaitable de filtrer le trafic indésirable à la source pour empêcher la transmission de trafic qui consomme de la bande passante. |
| **Simplicité de configuration** | •Il peut être plus facile d'implémenter une liste ACL à destination, mais le trafic utilisera inutilement la bande passante.<br>•Une liste de contrôle d'accès étendue peut être utilisée sur chaque routeur d'où provient le trafic. Cela permet d'économiser de la bande passante en filtrant le trafic à la source, mais exige de créer des listes de contrôle d'accès étendues sur plusieurs routeurs. |

# Exemple d'emplacement de liste de contrôle d'accès standard

Sur la figure, l'administrateur souhaite empêcher le trafic provenant du réseau 192.168.10.0/24 d'accéder au réseau 192.168.30.0/24.

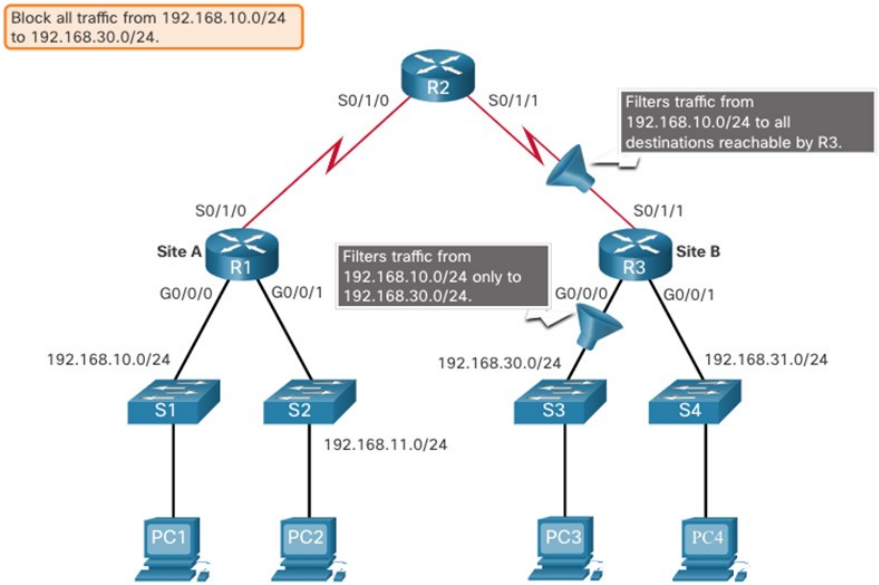
En suivant les instructions de placement de base, l'administrateur place une liste ACL standard sur le routeur R3.



# Exemple d'emplacement de liste de contrôle d'accès standard (Suite)

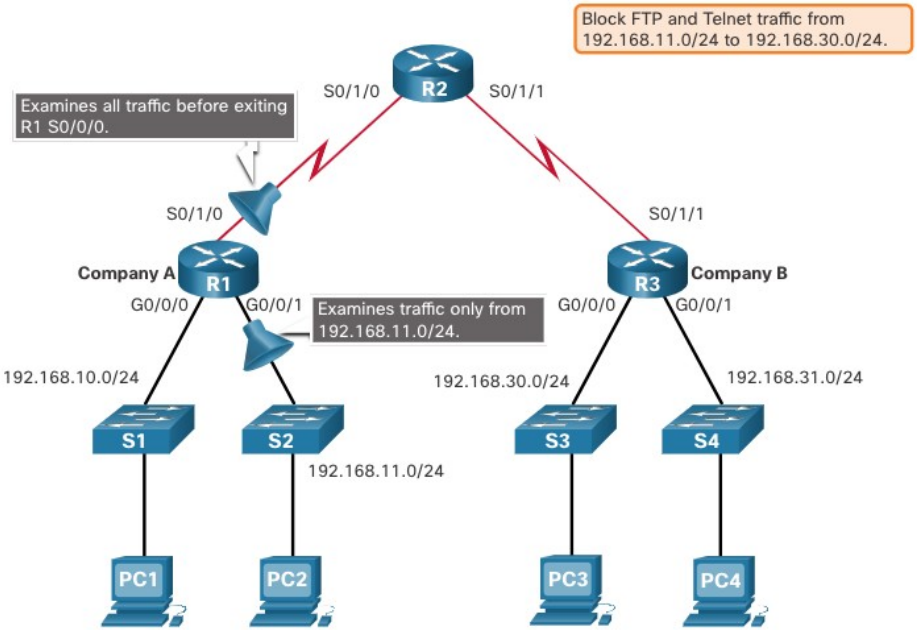
Il existe deux interfaces possibles sur R3 pour appliquer l'ACL standard:

- **Interface R3 S0/1/1 (entrante)** - L'ACL standard peut être appliquée entrante sur l'interface R3 S0/1/1 pour refuser le trafic à partir du réseau .10. Cependant, il filtre également le trafic .10 vers le réseau 192.168.31.0/24 (.31 dans cet exemple). Par conséquent, l'ACL standard ne doit pas être appliquée à cette interface.
- **Interface R3 G0/0 (sortante)** - L'ACL standard peut être appliquée sortante sur l'interface R3 G0/0/0. Cela n'affecte pas les autres réseaux accessibles par R3. Les paquets du réseau .10 pourront toujours atteindre le réseau .31. C'est la meilleure interface pour placer la liste ACL standard pour répondre aux exigences de trafic.



# Exemple d'emplacement d'une liste de contrôle d'accès étendue

- Les ACL étendus doivent être situés aussi près que possible de la source.
- Cependant, l'organisation ne peut placer des ACL que sur les appareils qu'elle contrôle. Par conséquent, cet emplacement doit être déterminé par la portée du contrôle dont dispose l'administrateur réseau.
- Dans la figure, par exemple, la société A veut refuser le trafic Telnet et FTP au réseau 192.168.30.0/24 de la société B à partir de son réseau 192.168.11.0/24 tout en autorisant tout autre trafic.



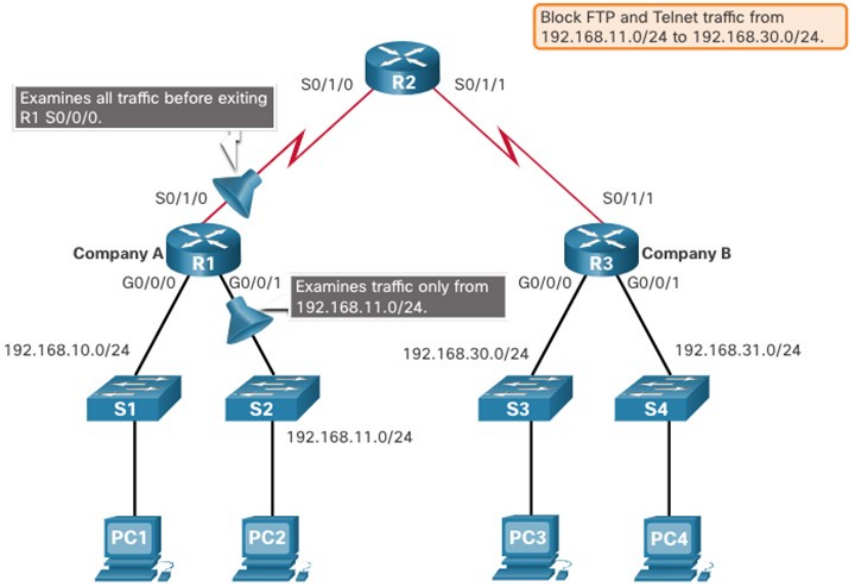
# Exemple d'emplacement d'une liste de contrôle d'accès étendue (Suite)

Un ACL étendu sur R3 permettrait d'accomplir la tâche, mais l'administrateur ne contrôle pas R3. En outre, cette solution autorise le passage du trafic indésirable sur l'ensemble du réseau avant de le bloquer lorsqu'il arrive à destination.

La solution consiste à placer une liste ACL étendue sur R1 qui spécifie à la fois les adresses source et de destination.

La figure illustre deux interfaces possibles sur R1 pour appliquer la liste de contrôle d'accès étendue:

- **interface R1 S0/1/0 (sortante)** - L'ACL étendue peut être appliquée sortante sur l'interface S0/1/0 Cette solution traitera tous les paquets quittant R1 y compris les paquets de 192.168.10.0/24.
- **Interface R1 G0/0/1 (entrante)** - L'ACL étendu peut être appliqué en entrée sur le G0/0/1 et seuls les paquets du réseau 192.168.11.0/24 sont soumis au traitement ACL sur R1 Puisque le filtre doit être limité aux seuls paquets quittant le réseau 192.168.11.0/24, l'application de la liste de contrôle d'accès étendue à G0/1 constitue la meilleure solution.




CISCO