Fiche de révision sur les ACL

Définition et Importance des ACL

- Les **ACL (Access Control List)**, ou **listes de contrôle d'accès**, sont des ensembles de règles appliquées aux interfaces des routeurs pour filtrer le trafic réseau.
- Elles permettent de déterminer quels paquets sont autorisés à transiter et lesquels doivent être bloqués, en fonction de critères tels que l'adresse IP source et de destination, le protocole et les ports.
- Le routeur examine l'en-tête de chaque paquet et le compare aux règles de l'ACL pour prendre une décision.
- Les ACL contribuent à :
  - **Maîtriser le réseau** en contrôlant le type de trafic autorisé.
  - **Améliorer la sécurité** en limitant l'accès à certaines parties du réseau.
  - **Optimiser le réseau** en gérant la bande passante et en appliquant des politiques spécifiques.

Types d'ACL

- **ACL Standards (1-99, 1300-1999) :**
  - Filtrage basé uniquement sur l'adresse IP source du paquet.
  - Utilisées pour autoriser ou interdire l'accès à un segment de réseau ou à une machine spécifique.
- **ACL Étendues (100-199, 200-2699) :**
  - Offrent un filtrage plus précis en examinant davantage de champs dans l'en-tête du paquet(adresses IP source et destination, protocoles, ports).
  - Permettent de contrôler des services spécifiques, comme le FTP ou le HTTP, en utilisant les numéros de port.
- **ACL Nommées :**
  - Similaire aux ACL standards et étendues, mais utilisent des noms au lieu de numéros pour les identifier, facilitant leur gestion.
  - Offrent plus de flexibilité avec des sous-commandes et des options d'édition.

Fonctionnement des ACL

- **Logique de première correspondance :** le routeur évalue les paquets en suivant l'ordre des règles dans l'ACL. Dès qu'une correspondance est trouvée, l'action associée à cette règle est appliquée, et le processus s'arrête.
- **Refus implicite :** si un paquet ne correspond à aucune règle de l'ACL, il est automatiquement rejeté.
- **Masque générique (Wildcard Mask) :** utilisé pour définir des plages d'adresses IP dans les règles de l'ACL.
  - Un 0 dans le masque indique que l'octet correspondant de l'adresse IP doit être comparé.
  - Un 255 indique que l'octet peut prendre n'importe quelle valeur.

Placement des ACL

- **ACL standards :** placées au plus proche de la destination, car elles sont plus restrictives.
- **ACL étendues :** placées au plus proche de la source, car elles filtrent au niveau de la couche 4 et permettent d'optimiser le trafic réseau.

Configuration des ACL (Exemples)

Les sources fournissent de nombreux exemples de configuration d'ACL sur des routeurs Cisco, illustrant :

- La création d'ACL standards et étendues.
- L'utilisation de masques génériques.
- Le blocage de protocoles spécifiques (ICMP pour le ping, TCP pour le FTP et le HTTP).
- La spécification de ports TCP/UDP.
- L'application d'ACL aux interfaces entrantes et sortantes des routeurs.

Conclusion

Les ACL sont un outil puissant pour contrôler et sécuriser un réseau. Elles permettent de filtrer le trafic aux niveaux 3 et 4 du modèle OSI. En complément des ACL, des techniques de filtrage applicatif au niveau de la couche 7 (proxy) peuvent être mises en place pour une sécurité renforcée.

Résumé des commandes de base pour les ACL Cisco

Les sources fournies offrent une description détaillée de la configuration des ACL (Access Control Lists) sur les routeurs Cisco, avec des exemples pratiques. Voici un résumé des commandes de base pour créer et appliquer des ACL :

1. Accéder au mode de configuration globale :

```
Router> enable
Router# configure terminal
```

2. Créer une ACL standard (numéros 1-99, 1300-1999) :

```
Router(config)# access-list [numéro_acl] [permit | deny]
[adresse_ip_source] [masque_générique]
```

- `[numéro_acl]` : Identifiant numérique de l'ACL.
- `[permit | deny]` : Indique si l'ACL doit autoriser ou refuser le trafic correspondant.
- `[adresse_ip_source]` : Adresse IP source à filtrer.
- `[masque_générique]` : Masque générique pour spécifier la plage d'adresses IP source.

Exemple :

```
Router(config)# access-list 1 deny 10.1.2.0 0.0.0.255
```

Cette règle refuse tout le trafic provenant du réseau 10.1.2.0/24.

3. Créer une ACL étendue (numéros 100-199, 200-2699) :

```
Router(config)# access-list [numéro_acl] [permit | deny] [protocole]
[adresse_ip_source] [masque_générique_source] [adresse_ip_destination]
[masque_générique_destination] [options]
```

- `[protocole]` : Protocole à filtrer (ex: tcp, udp, icmp).
- `[options]` : Options de filtrage supplémentaires, comme le numéro de port (`eq` pour égal, `gt` pour supérieur à, `lt` pour inférieur à).

Exemple :

```
Router(config)# access-list 100 deny icmp 10.1.3.0 0.0.0.255 10.1.2.0
0.0.0.255
```

Cette règle refuse les paquets ICMP (ping) provenant du réseau 10.1.3.0/24 vers le réseau 10.1.2.0/24.

4. Créer une ACL nommée :

```
Router(config)# ip access-list extended [nom_acl]
```

- `[nom_acl]` : Nom descriptif de l'ACL.

Exemple :

```
R2(config)# ip access-list extended David-HTTP
```

5. Ajouter des règles à une ACL nommée :

```
Router( config-ext-nacl )#[deny | permit] [protocole] [source]
[destination] [options]
```

- `[source]` : Adresse IP source ou mot-clé `any`.
- `[destination]` : Adresse IP de destination ou mot-clé `any`.

Exemple :

```
R2( config-ext-nacl )# deny tcp host 172.16.3.10 host 172.16.1.100 eq www
```

Cette règle refuse le trafic TCP provenant de l'hôte 172.16.3.10 vers l'hôte 172.16.1.100 sur le port `www` (80).

6. Appliquer une ACL à une interface :

```
Router(config)# interface [nom_interface]
Router(config-if)# ip access-group [numéro_acl | nom_acl] [in | out]
```

- `[nom_interface]` : Nom de l'interface du routeur (ex: GigabitEthernet0/0).
- `[in | out]` : Indique si l'ACL doit être appliquée aux paquets entrants ou sortants de l'interface.

Exemple :

```
Router(config-if)# ip access-group 100 in
```

Cette commande applique l'ACL numéro 100 aux paquets entrants de l'interface.

Note : Les commandes présentées ci-dessus sont des exemples de base. Les sources fournies présentent des configurations plus complexes, avec l'utilisation de différents protocoles, ports et options de filtrage. Il est recommandé de consulter les sources pour approfondir vos connaissances sur les ACL Cisco.