TP - Configuration des Filtres ACL

Objectif :

L'objectif de ce TP est de configurer un filtre ACL sur un routeur Cisco dans Cisco Packet Tracer pour bloquer le trafic en provenance d'un hôte spécifique avec une adresse IP donnée (par exemple, 12.0.0.100).

Objectifs

L'objectif de ce TP est de configurer et de tester des filtres ACL dans un environnement Cisco Packet Tracer. Le but est de bloquer le trafic IP en provenance d'un hôte spécifique (par exemple, ayant pour adresse IP 12.0.0.100) sur un réseau simulé.

Étapes de Configuration

1. Configuration de base sur Cisco Packet Tracer

- Ajoutez les périphériques suivants dans votre simulation :
  - Routeur (Router0)
  - Commutateur (Switch0)
  - Deux hôtes (PC0 et PC1)

Assurez-vous que ces périphériques sont connectés entre eux et que le réseau fonctionne correctement avant d'appliquer le filtrage ACL.

2. Connexion au routeur

- Accédez à la console du routeur :
  - Clic droit sur le routeur dans Cisco Packet Tracer, puis cliquez sur "Console" pour ouvrir la console du routeur.

3. Configuration de l'adresse IP du routeur

Configurez l'adresse IP du routeur sur l'interface qui connecte le réseau local (LAN) à 12.0.0.1.

Par exemple, sur l'interface FastEthernet0/0 :

```
Router> enable
Router# configure terminal
Router(config)# interface GigabitEthernet0/0/0
Router(config-if)# ip address 12.0.0.1 255.0.0.0
Router(config-if)# no shutdown
Router(config-if)# exit
```

4. Création d'une ACL étendue

Créez une ACL étendue pour filtrer le trafic provenant de l'hôte ayant l'adresse IP 12.0.0.100.

Nous allons bloquer tout le trafic provenant de cette adresse IP.

```
Router(config)# ip access-list extended Block_IP_12.0.0.100
Router(config-ext-nacl)# deny ip host 12.0.0.100 any
Router(config-ext-nacl)# permit ip any any
Router(config-ext-nacl)# exit
```

5. Application de l'ACL sur l'interface

Appliquez cette ACL à l'interface où vous souhaitez filtrer le trafic entrant (par exemple, FastEthernet0/0). Cela permettra de bloquer le trafic provenant de l'adresse IP 12.0.0.100 sur cette interface.

```
Router(config)# interface FastEthernet0/0
Router(config-if)# ip access-group Block_IP_12.0.0.100 in
Router(config-if)# exit
```

6. Test avant l'application du filtre

Avant d'appliquer l'ACL, vous pouvez tester la connectivité entre les hôtes pour vérifier que tout fonctionne bien. Utilisez la commande ping depuis PC0 vers PC1 :

- PC0 (adresse IP 12.0.0.100) ping vers PC1 (adresse IP 12.0.0.17) :

```
PC0> ping 12.0.0.17
Reply from 12.0.0.17: bytes=32 time<1ms TTL=255
```

7. Test après application du filtre

Une fois l'ACL appliquée, les paquets en provenance de PC0 (avec l'adresse IP 12.0.0.100) devraient être bloqués. Vous pouvez effectuer un ping depuis PC0 vers PC1 :

- PC0 (adresse IP 12.0.0.100) ping vers PC1 (adresse IP 12.0.0.17) :

```
PC0> ping 12.0.0.17
Request Timed Out
```

Ce résultat montre que le trafic en provenance de 12.0.0.100 a bien été bloqué.

8. Vérification de la configuration de l'ACL

Pour vérifier que l'ACL est correctement configurée et appliquée, utilisez la commande suivante sur le routeur :

```
Router# show access-lists
```

Cela vous permettra de voir l'état de votre ACL, notamment les règles de filtrage (par exemple, deny pour 12.0.0.100).

9. Suppression de l'ACL

Si vous souhaitez supprimer l'ACL de l'interface pour restaurer la connectivité, vous pouvez utiliser les commandes suivantes :

```
Router(config)# interface FastEthernet0/0
Router(config-if)# no ip access-group Block_IP_12.0.0.100 in
Router(config-if)# exit
```

10. Test après suppression du filtre

Après avoir supprimé l'ACL de l'interface, effectuez à nouveau un ping depuis PC0 vers PC1. Cette fois, le trafic devrait être autorisé, et vous devriez recevoir une réponse :

```
PC0> ping 12.0.0.17
Reply from 12.0.0.17: bytes=32 time<1ms TTL=255
```

Conclusion

Ce TP montre comment configurer une ACL étendue sur un routeur Cisco dans Cisco Packet Tracer pour filtrer le trafic IP. Les ACL sont une fonctionnalité essentielle pour sécuriser un réseau en contrôlant quels paquets peuvent entrer ou sortir d'un réseau en fonction de critères définis, comme l'adresse IP source ou destination.