Packet Tracer - Démonstration de la liste de contrôle d'accès

Objectifs

Partie 1: Vérifier la connectivité locale et tester la liste de contrôle d'accès

Partie 2: Supprimer la liste de contrôle d'accès et répéter le test

# Contexte

Dans cet exercice, vous allez observer comment une liste de contrôle d'accès peut être utilisée pour empêcher une requête ping d'atteindre les hôtes sur des réseaux distants. Après le retrait de la liste de contrôle d'accès de la configuration, les requêtes ping aboutiront.

# Table d'adressage

|  |  |  |
| --- | --- | --- |
| Appareil | Interface | Adresse IP / Préfixe |
| R1 | G0/0 | 192.168.10.1/24 |
| R1 | G0/1 | 192.168.11.1/24 |
| R1 | S0/0/0 | 10.1.1.1/30 |
| R2 | S0/0/0 | 10.10.1.2/30 |
| R2 | S0/0/1 | 10.10.1.5/30 |
| R3 | G0/0 | 192.168.30.1/24 |
| R3 | G0/1 | 192.168.31.1/24 |
| R3 | S0/0/1 | 10.10.1.6/24 |
| PC1 | Carte réseau | 192.168.10.10/24 |
| PC2 | Carte réseau | 192.168.10.11/24 |
| PC3 | Carte réseau | 192.168.11.10/24 |
| PC4 | Carte réseau | 192.168.30.12/24 |
| Serveur DNS | Carte réseau | 192.168.31.12/24 |

# Instructions

## Vérifier la connectivité locale et tester la liste de contrôle d'accès

### Envoyez une requête ping au réseau local pour vérifier la connectivité.

* + - 1. À partir de l'invite de commande de **PC1**, envoyez une requête ping à **PC2**.
      2. À partir de l'invite de commande de **PC1**, envoyez une requête ping à **PC3**.

#### Question:

Pourquoi les requêtes ping ont-elles abouti?

### Envoyez une requête ping aux périphériques des réseaux distants pour tester le fonctionnement des listes de contrôle d'accès.

* + - 1. À partir de l'invite de commande de **PC1**, envoyez une requête ping à **PC4**.
      2. À partir de l'invite de commande de **PC1**, envoyez une requête ping à **DNS Server**.

#### Question:

Pourquoi les requêtes ping ont-elles échoué? (**Conseil**: Utilisez le mode de simulation ou afficher les configurations des routeurs pour investiguer.

## Supprimer la liste de contrôle d'accès et répéter le test

### Utilisez les commandes show pour examiner la configuration de la liste de contrôle d'accès.

* + - 1. Accédez à l'interface de ligne de commande R1. Utilisez les commandes **show run** et **show access-lists** pour afficher les listes de contrôle d'accès actuellement configurées. Pour afficher rapidement les listes de contrôle d'accès actuelles, utilisez **show access-lists**. Entrez la commande **show access-lists** suivie d'un espace et d'un point d'interrogation (?) pour afficher les options disponibles:

Ouvrez la fenêtre de configuration.

R1# **show access-lists ?**

<1-199> ACL number

WORD ACL name

<cr>

Si vous connaissez le numéro ou le nom de la liste de contrôle d'accès, vous pouvez limiter davantage les résultats de la commande **show**. Toutefois, **R1** a une seule liste de contrôle d'accès. Par conséquent, la commande **show access-lists** suffira.

R1#**show access-lists**

Standard IP access list 11

10 deny 192.168.10.0 0.0.0.255

20 permit any

La première ligne de l'ACL bloque tout paquet provenant du réseau **192.168.10.0/24** , qui comprend les échos du protocole ICMP(Internet Control Message Protocol) (requêtes ping). La deuxième ligne de la liste ACL permet à tous les autres trafics **IP** provenant de **n'importe quelle** source de traverser le routeur.

* + - 1. Pour que la liste ACL influence le fonctionnement du routeur, elle doit être appliquée à une interface dans une direction définie. Dans ce scénario, la liste ACL est utilisée pour filtrer le trafic sortant d’une interface. Par conséquent, chaque trafic provenant de l’interface spécifiée du routeur R1 sera inspecté selon ACL 11.

Bien que vous puissiez voir les informations IP avec la commande **show ip interface**, dans certaines situations il est plus judicieux d'utiliser simplement la commande **show run**. Pour obtenir une liste complète des interfaces auxquelles la liste ACL pouvant être appliquée et la liste de toutes les ACL configurées, utilisez la commande suivante:

R1# **show run | inclure l'interface|access**

interface GigabitEthernet0/0

interface GigabitEthernet0/1

interface Serial0/0/0

ip access-group 11 out

interface Serial0/0/1

interface Vlan1

access-list 11 deny 192.168.10.0 0.0.0.255

access-list 11 permit any

Le deuxième symbole de tube «|» crée une condition OR qui correspond à 'interface' OU 'access '. Il est important qu'aucun espace ne soit inclus dans la condition OR. Utilisez l'une de ces commandes ou les deux pour trouver des informations sur l'ACL.

#### Question:

À quelle interface et dans quelle direction l'ACL est-elle appliquée?

### Supprimez la liste de contrôle d'accès 11 de la configuration.

Vous pouvez supprimer des listes de contrôle d'accès de la configuration en exécutant la commande **no access list** *[numéro de la liste de contrôle d'accès]*. La commande **no access-list** permet de supprimer toutes les listes ACL configurées sur le routeur. La commande **no access-list** [*number of the ACL*] permet de supprimer uniquement une liste ACL précise. La suppression d'une liste ACL d'un routeur ne supprime pas l'ACL de l'interface. La commande qui applique l'ACL à l'interface doit être supprimée séparément.

* + - 1. Sous l'interface Serial0/0/0, supprimer la liste d'accès 11, qui était auparavant appliquée à l'interface en tant que filtre **outgoing** :

R1(config)# **interface s0/0/0**

R1(config-if)# **no ip access-group 11 out**

* + - 1. En mode de configuration globale, supprimez la liste de contrôle d'accès en tapant la commande suivante:

R1(config)# **no access-list 11**

* + - 1. Vérifiez que le **PC1** peut maintenant envoyer une requête ping vers le **serveur DNS** et vers le **PC4.**