Packet Tracer - Configurer les ACLs IPv4 standard nommées

Table d'adressage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appareil | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| R1 | F0/0 | 192.168.10.1 | 255.255.255.0 | N/A |
| *R1* | F0/1 | 192168.20,1 | 255.255.255.0 | N/A |
| *R1* | E0/0/0 | 192.168.100.1 | 255.255.255.0 | N/A |
| *R1* | E0/1/0 | 192.168.200.1 | 255.255.255.0 | N/A |
| Serveur de fichiers | Carte réseau | 192.168.200.100 | 255.255.255.0 | 192.168.200.1 |
| Serveur Web | Carte réseau | 192.168.100.100 | 255.255.255.0 | 192.168.100.1 |
| PC0 | Carte réseau | 192.168.20.3 | 255.255.255.0 | 192168.20,1 |
| PC1 | Carte réseau | 192.168.20.4 | 255.255.255.0 | 192168.20,1 |
| PC2 | Carte réseau | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |

# Objectifs

Partie 1 : configuration et application d'une liste de contrôle d'accès standard nommée

Partie 2 : vérification de l'implémentation de la liste de contrôle d'accès

# Contexte/scénario

L’administrateur réseau principal vous a chargé de créer une liste ACL standard nommée afin d’empêcher l’accès au serveur de fichiers. Le serveur de fichiers contient la base de données des applications Web. Seules la station de travail Web Manager PC1 et le serveur Web doivent accéder au serveur de fichiers. Tout autre trafic vers le serveur de fichiers doit être refusé.

# Instructions

## Configuration et application d'une liste de contrôle d'accès standard nommée

### Vérifiez la connectivité avant de configurer et d'appliquer la liste de contrôle d'accès.

Les trois postes de travail devraient être capables de faire un ping à la fois sur le **serveur Web** et sur le **serveur de fichiers**.

### Configurez une liste de contrôle d'accès standard nommée.

Ouvrez la fenêtre de configuration.

* + - 1. Configurez la liste de contrôle d'accès nommée suivante sur **R1**.

R1(config)# **ip access-list standard File\_Server\_Restrictions**

R1(config-std-nacl)# **permit host 192.168.20.4**

R1(config-std-nacl)# **permit host 192.168.100.100**

R1(config-std-nacl)# **deny any**

**Remarque**: À des fins de notation, le nom ACL respecte la casse et les instructions doivent être dans le même ordre que celui indiqué.

* + - 1. Utilisez la commande **show access-lists** pour vérifier le contenu de la liste d'accès avant de l'appliquer à une interface. Assurez-vous que vous n'avez pas mal tapé les adresses IP et que les instructions sont dans le bon ordre.

R1# **show access-lists**

Standard IP access list File\_Server\_Restrictions

10 permit host 192.168.20.4

20 permit host 192.168.100.100

30 deny any

### Appliquez la liste de contrôle d'accès nommée.

* + - 1. Appliquez l'ACL en sortie sur l'interface Fast Ethernet 0/1.

**Remarque** : Dans un réseau opérationnel réel, l'application d'une liste d'accès à une interface active n'est pas une bonne pratique et devrait être évitée si possible.

R1(config-if)# **ip access-group File\_Server\_Restrictions out**

* + - 1. Enregistrer la configuration.

Fermez la fenêtre de configuration.

## Vérification de l'implémentation de la liste de contrôle d'accès

### Vérifiez la configuration de la liste de contrôle d'accès et son application à l'interface.

Ouvrez la fenêtre de configuration.

Utilisez la commande **show access-lists** pour vérifier la configuration de la liste de contrôle d'accès. Utilisez la commande **show run** ou **show ip interface fastethernet 0/1** pour vérifier que la liste de contrôle d'accès est appliquée correctement à l'interface.

### Vérifiez que la liste de contrôle d'accès fonctionne convenablement.

Les trois postes de travail devraient pouvoir envoyer un ping au **serveur Web**, mais seuls le **PC1** et le **serveur Web** devraient pouvoir envoyer un ping au **serveur de fichiers**. Répétez la commande **show access-lists** pour voir le nombre de paquets correspondant à chaque instruction.