Packet Tracer – Configurer des listes ACL IPv4 standard numérotées

Topologie

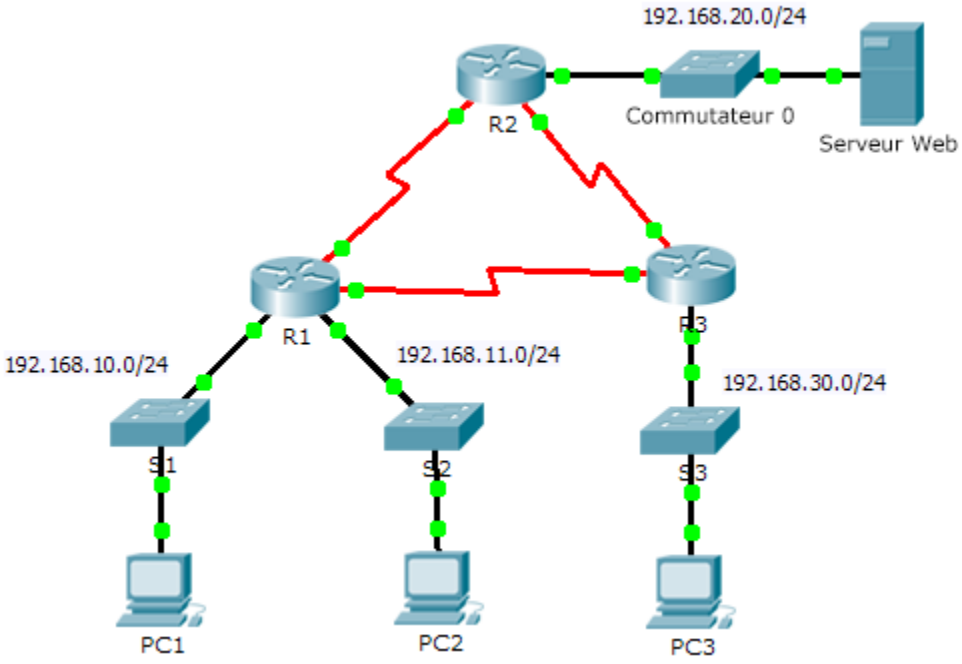

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	192.168.10.1	255.255.255.0	N/A
	G0/1	192.168.11.1	255.255.255.0	N/A
	S0/0/0	10.1.1.1	255.255.255.252	N/A
	S0/0/1	10.3.3.1	255.255.255.252	N/A
R2	G0/0	192168.20,1	255.255.255.0	N/A
	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
R3	G0/0	192.168.30.1	255.255.255.0	N/A
	S0/0/0	10.3.3.2	255.255.255.252	N/A
	S0/0/1	10.2.2.2	255.255.255.252	N/A
PC1	Carte réseau	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Carte réseau	192.168.11.10	255.255.255.0	192.168.11.1
PC3	Carte réseau	192.168.30.10	255.255.255.0	192.168.30.1
WebServer	Carte réseau	192.168.20.254	255.255.255.0	192168.20,1

Objectifs

Partie 1 : planification d'une implémentation de liste de contrôle d'accès

Partie 2 : configuration, application et vérification d'une liste de contrôle d'accès standard

Contexte/scénario

Les listes de contrôle d'accès standard sont des scripts de configuration de routeur déterminant l'autorisation ou le rejet de paquets en fonction de leur adresse source. Cet exercice porte sur la définition de critères de filtrage, sur la configuration de listes de contrôle d'accès standard, sur l'application de listes de contrôle d'accès aux interfaces des routeurs et sur la vérification et le test de la mise en œuvre de listes de contrôle d'accès. Les routeurs sont déjà configurés, y compris le routage d'adresses IP et de protocole EIGRP (Enhanced Interior Gateway Routing Protocol).

Partie 1 : Planification d'une implémentation de liste de contrôle d'accès

Étape 1 : Étudiez la configuration réseau actuelle.

Avant d'appliquer une liste de contrôle d'accès à un réseau, il convient de vérifier que vous disposez d'une connectivité complète. Vérifiez la connectivité complète du réseau en choisissant un PC et en envoyant une requête ping à d'autres périphériques sur le réseau. Chaque requête ping doit aboutir.

Étape 2 : Évaluez deux stratégies réseau et planifiez les implémentations de liste de contrôle d'accès.

a. Les stratégies réseau suivantes sont implémentées sur **R2** :

- Le réseau 192.168.11.0/24 n'est pas autorisé à accéder à **WebServer** situé sur le réseau 192.168.20.0/24.
- Tous les autres accès sont autorisés.

Pour limiter l'accès du réseau 192.168.11.0/24 vers **WebServer** sur 192.168.20.254 sans perturber le reste du trafic, il faut créer une liste de contrôle d'accès sur **R2**. Cette liste d'accès doit être placée sur l'interface de sortie vers **WebServer**. Une deuxième règle doit être créée sur **R2** pour autoriser tous les autres types de trafic.

b. Les stratégies réseau suivantes sont implémentées sur **R3** :

- Le réseau 192.168.10.0/24 n'est pas autorisé à communiquer avec le réseau 192.168.30.0/24.
- Tous les autres accès sont autorisés.

Une liste d'accès doit être créée sur le routeur **R3** afin de limiter l'accès du réseau 192.168.10.0/24 au réseau 192.168.30/24 sans perturber les autres trafics. Il faut placer la liste ACL sur l'interface sortante vers **PC3**. Une deuxième règle doit être créée sur **R3** pour autoriser tous les autres types de trafic.

Partie 2 : Configuration, application et vérification d'une liste de contrôle d'accès standard

Étape 1 : Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R2.

a. Créez une liste de contrôle d'accès en utilisant le numéro 1 sur **R2** avec une instruction refusant l'accès vers le réseau 192.168.20.0/24 à partir du réseau 192.168.11.0/24.

```
R2(config)# access-list 1 deny 192.168.11.0 0.0.0.255
```

b. Par défaut, une liste d'accès refuse tout trafic non conforme aux règles. Pour autoriser tout autre trafic, configurez l'instruction suivante :

```
R2(config)# access-list 1 permit any
```

c. Pour que la liste de contrôle d'accès filtre réellement le trafic, elle doit être appliquée au routeur. Appliquez la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet 0/0.

```
R2(config)# interface GigabitEthernet0/0
R2(config-if)# ip access-group 1 out
```

Étape 2 : Configurez et appliquez une liste de contrôle d'accès standard numérotée sur R3.

a. Créez une liste de contrôle d'accès en utilisant le numéro 1 sur **R3** avec une instruction refusant l'accès au réseau 192.168.30.0/24 à partir du réseau du **PC1** (192.168.10.0/24).

```
R3(config)# access-list 1 deny 192.168.10.0 0.0.0.255
```

b. Par défaut, une liste ACL refuse tout trafic non conforme aux règles. Pour autoriser tout autre trafic, créez une deuxième règle pour la liste de contrôle d'accès ACL 1.

```
R3(config)# access-list 1 permit any
```

c. Appliquez la liste de contrôle d'accès en la plaçant pour le trafic sortant sur l'interface Gigabit Ethernet 0/0.

```
R3(config)# interface GigabitEthernet0/0
R3(config-if)# ip access-group 1 out
```

Étape 3 : Vérifiez la configuration et le fonctionnement des listes de contrôle d'accès.

a. Sur les routeurs **R2** et **R3**, entrez la commande **show access-list** pour vérifier les configurations des listes ACL. Utilisez la commande **show run** ou **show ip interface gigabitethernet 0/0** pour vérifier que les listes de contrôle d'accès sont placées correctement.

b. Avec les deux listes de contrôle d'accès en place, le trafic réseau est limité en fonction des stratégies détaillées dans la Partie 1. Utilisez les tests suivants pour vérifier les implémentations de liste de contrôle d'accès :

- Une requête ping de 192.168.10.10 vers 192.168.11.10 aboutit.
- Une requête ping de 192.168.10.10 vers 192.168.20.254 aboutit.
- Une requête ping de 192.168.11.10 vers 192.168.20.254 échoue.
- Une requête ping de 192.168.10.10 vers 192.168.30.10 échoue.
- Une requête ping de 192.168.11.10 vers 192.168.30.10 aboutit.
- Une requête ping de 192.168.30.10 vers 192.168.20.254 aboutit.