Exercice PT 5.3.4 : configuration de listes de contrôle d'accès étendues

Diagramme de topologie

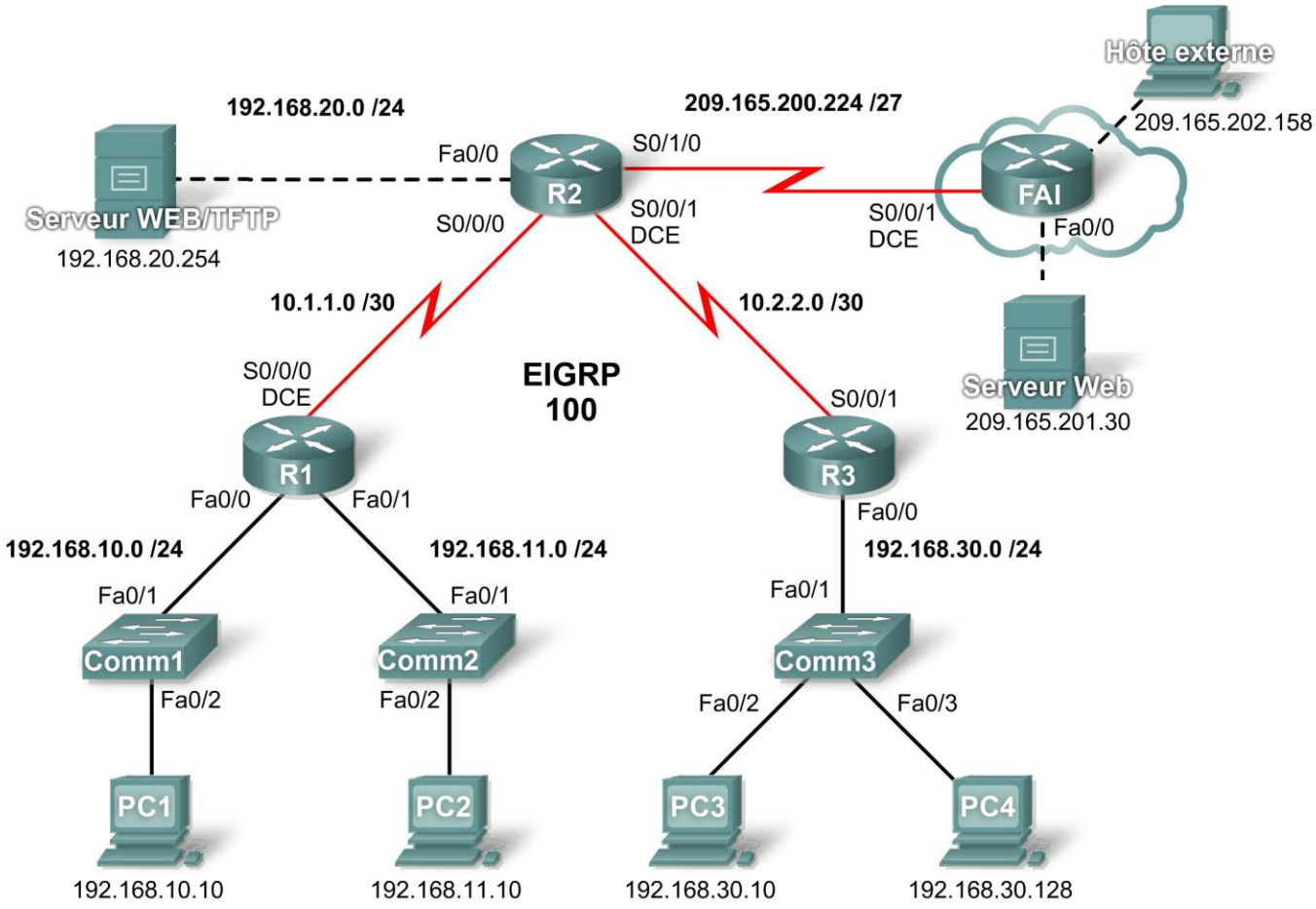

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau
R1	**S0/0/0**	10.1.1.1	255.255.255.252
	Fa0/0	192.168.10.1	255.255.255.0
	Fa0/1	192.168.11.1	255.255.255.0
R2	**S0/0/0**	10.1.1.2	255.255.255.252
	S0/0/1	10.2.2.2	255.255.255.252
	S0/1/0	209.165.200.225	255.255.255.224
	Fa0/0	192.168.20.1	255.255.255.0
R3	**S0/0/1**	10.2.2.1	255.255.255.252
	Fa0/0	192.168.30.1	255.255.255.0
FAI	**S0/0/1**	209.165.200.226	255.255.255.224
	Fa0/0	209.165.201.1	255.255.255.224
	Fa0/1	209.165.202.129	255.255.255.224
PC1	**Carte réseau**	192.168.10.10	255.255.255.0
PC2	**Carte réseau**	192.168.11.10	255.255.255.0
PC3	**Carte réseau**	192.168.30.10	255.255.255.0
PC4	**Carte réseau**	192.168.30.128	255.255.255.0
Serveur TFTP/Web	**Carte réseau**	192.168.20.254	255.255.255.0
Serveur Web	**Carte réseau**	209.165.201.30	255.255.255.224
Hôte externe	**Carte réseau**	209.165.202.158	255.255.255.224

Objectifs pédagogiques

- Étudier la configuration actuelle du réseau
- Évaluer une stratégie de réseau et planifier la mise en œuvre de listes de contrôle d'accès
- Configurer des listes de contrôle d'accès étendues numérotées
- Configurer des listes de contrôle d'accès étendues nommées

Présentation

Les listes de contrôle d'accès étendues sont des scripts de configuration du routeur qui définissent si celui-ci autorise ou refuse des paquets selon l'adresse source ou de destination, ainsi qu'en fonction de protocoles ou de ports. Les listes de contrôle d'accès étendues offrent une meilleure souplesse et une plus grande précision que les listes de contrôle d'accès standard. Cet exercice porte principalement sur la définition de critères de filtrage, la configuration de listes de contrôle d'accès étendues, l'application de ces listes aux interfaces des routeurs, ainsi que sur la vérification et le test de leur mise en œuvre. Les routeurs sont déjà configurés, notamment les adresses IP et le routage EIGRP. Le mot de passe d'exécution utilisateur est **cisco** et le mot de passe d'exécution privilégié est **class**.

Tâche 1 : étude de la configuration actuelle du réseau

Étape 1. Affichage de la configuration en cours sur les routeurs

Affichez les configurations en cours sur les trois routeurs à l'aide de la commande **show running-config** en mode d'exécution privilégié. Remarquez que les interfaces et le routage sont entièrement configurés. Comparez les configurations d'adresses IP à la table d'adressage ci-dessus. Aucune liste de contrôle d'accès ne doit être configurée sur les routeurs à ce stade.

Aucune configuration du routeur FAI n'est nécessaire au cours de cet exercice. Il est supposé que vous n'êtes pas responsable du routeur FAI et que celui-ci est configuré et entretenu par l'administrateur FAI.

Étape 2. Vérification que tous les périphériques ont accès à tous les autres emplacements

Avant d'appliquer des listes de contrôle d'accès à un réseau, il est important de vérifier que vous disposez d'une connectivité complète. Si vous ne testez pas la connectivité de votre réseau avant d'appliquer une liste de contrôle d'accès, le dépannage sera plus difficile.

Afin de garantir la connectivité sur tout le réseau, utilisez les commandes **ping** et **tracert** entre les différents périphériques réseau pour vérifier les connexions.

Tâche 2 : évaluation d'une stratégie de réseau et planification de la mise en œuvre de listes de contrôle d'accès

Étape 1. Évaluation de la stratégie pour les réseaux locaux de R1

- Pour le réseau 192.168.10.0/24, bloquez l'accès Telnet vers tous les emplacements et l'accès TFTP au serveur Web/TFTP d'entreprise à l'adresse 192.168.20.254. Tout autre accès est autorisé.
- Pour le réseau 192.168.11.0/24, autorisez l'accès TFTP et l'accès Web au serveur Web/TFTP d'entreprise à l'adresse 192.168.20.254. Bloquez tout autre trafic en provenance du réseau 192.168.11.0/24 vers le réseau 192.168.20.0/24. Tout autre accès est autorisé.

Étape 2. Planification de la mise en œuvre des listes de contrôle d'accès pour les réseaux locaux de R1

- Deux listes de contrôle d'accès permettent de mettre en œuvre intégralement la stratégie de sécurité pour les réseaux locaux de R1.
- La première liste prend en charge la première partie de la stratégie et est configurée sur R1 et appliquée en entrée de l'interface Fast Ethernet 0/0.
- La seconde liste prend en charge la seconde partie de la stratégie et est configurée sur R1 et appliquée en entrée de l'interface Fast Ethernet 0/1.

Étape 3. Évaluation de la stratégie pour le réseau local de R3

- L'accès aux adresses IP du réseau 192.168.20.0/24 est bloqué pour toutes les adresses IP du réseau 192.168.30.0/24.
- La première moitié du réseau 192.168.30.0/24 a accès à toutes les destinations.
- La seconde moitié du réseau 192.168.30.0/24 a accès aux réseaux 192.168.10.0/24 et 192.168.11.0/24.
- La seconde moitié du réseau 192.168.30.0/24 dispose d'un accès Web et ICMP à toutes les autres destinations.
- Tout autre accès est implicitement refusé.

Étape 4. Planification de la mise en œuvre des listes de contrôle d'accès pour le réseau local de R3

Cette étape requiert la configuration d'une liste de contrôle d'accès sur R3, appliquée en entrée de l'interface Fast Ethernet 0/0.

Étape 5. Évaluation de la stratégie pour le trafic en provenance d'Internet via le fournisseur de services Internet (FAI)

- Les hôtes externes peuvent établir une session Web avec le serveur Web interne uniquement sur le port 80.
- Seules les sessions TCP établies sont autorisées en entrée.
- Seules les réponses ping sont autorisées via R2.

Étape 6. Planification de la mise en œuvre des listes de contrôle d'accès pour le trafic en provenance d'Internet via le fournisseur de services Internet (FAI)

Cette étape requiert la configuration d'une liste de contrôle d'accès sur R2, appliquée en entrée de l'interface Serial 0/1/0.

Tâche 3 : configuration de listes de contrôle d'accès étendues numérotées

Étape 1. Définition des masques génériques

Deux listes de contrôle d'accès sont nécessaires pour appliquer la stratégie de contrôle d'accès sur R1. Ces deux listes doivent être conçues pour refuser un réseau de classe C complet. Vous allez configurer un masque générique correspondant à tous les hôtes de chacun de ces réseaux de classe C.

Par exemple, pour l'intégralité du sous-réseau de 192.168.10.0/24 à associer, le masque générique est 0.0.0255. Cela peut être considéré comme « contrôler, contrôler, contrôler, ignorer » et correspond par définition au réseau 192.168.10.0/24 dans sa totalité.

Étape 2. Configuration de la première liste de contrôle d'accès étendue pour R1

En mode de configuration globale, configurez la première liste de contrôle d'accès avec le numéro 110. Vous souhaitez tout d'abord bloquer le trafic Telnet vers tout emplacement pour toutes les adresses IP du réseau 192.168.10.0/24.

Lorsque vous écrivez l'instruction, vérifiez que vous vous trouvez bien en mode de configuration globale.

```
R1(config)#access-list 110 deny tcp 192.168.10.0 0.0.0.255 any eq telnet
```

Bloquez ensuite pour toutes les adresses IP du réseau 192.168.10.0/24 l'accès TFTP à l'hôte à l'adresse 192.168.20.254.

```
R1(config)#access-list 110 deny udp 192.168.10.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Enfin, autorisez tout autre trafic.

```
R1(config)#access-list 110 permit ip any any
```

Étape 3. Configuration de la seconde liste de contrôle d'accès étendue pour R1

Configurez la seconde liste de contrôle d'accès avec le numéro 111. Autorisez l'accès www à l'hôte ayant l'adresse 192.168.20.254 à toute adresse IP du réseau 192.168.11.0/24.

```
R1(config)#access-list 111 permit tcp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq www
```

Autorisez ensuite l'accès TFTP à l'hôte ayant l'adresse 192.168.20.254 à toutes les adresses IP du réseau 192.168.11.0/24.

```
R1(config)#access-list 111 permit udp 192.168.11.0 0.0.0.255 host
192.168.20.254 eq tftp
```

Bloquez tout autre trafic en provenance du réseau 192.168.11.0/24 vers le réseau 192.168.20.0/24.

```
R1(config)#access-list 111 deny ip 192.168.11.0 0.0.0.255 192.168.20.0
0.0.0.255
```

Enfin, autorisez tout autre trafic. Cette instruction garantit que le trafic en provenance d'autres réseaux n'est pas bloqué.

```
R1(config)#access-list 111 permit ip any any
```

Étape 4. Vérification de la configuration des listes de contrôle d'accès

Pour confirmer les configurations sur R1, lancez la commande **show access-lists**. Le résultat doit être similaire à celui-ci :

```
R1#show access-lists
Extended IP access list 110
   deny tcp 192.168.10.0 0.0.0.255 any eq telnet
   deny udp 192.168.10.0 0.0.0.255 host 192.168.20.254 eq tftp
   permit ip any any
Extended IP access list 111
   permit tcp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq www
   permit udp 192.168.11.0 0.0.0.255 host 192.168.20.254 eq tftp
   deny ip 192.168.11.0 0.0.0.255 192.168.20.0 0.0.0.255
   permit ip any any
```

Étape 5. Application des instructions aux interfaces

Pour appliquer une liste de contrôle d'accès à une interface, passez en mode de configuration d'interface. Configurez la commande **ip access-group** *numéro-liste-accès* {**in** | **out**} pour appliquer la liste de contrôle d'accès à l'interface.

Chaque liste de contrôle d'accès filtre le trafic entrant. Appliquez la liste 110 à l'interface Fast Ethernet 0/0 et la liste 111 à l'interface Fast Ethernet 0/1.

```
R1(config)#interface fa0/0
R1(config-if)#ip access-group 110 in
R1(config-if)#interface fa0/1
R1(config-if)#ip access-group 111 in
```

Vérifiez que les listes de contrôle d'accès apparaissent dans la configuration en cours de R1 et qu'elles ont été appliquées aux interfaces correctes.

Étape 6. Test des listes de contrôle d'accès configurées sur R1

Une fois les listes de contrôle d'accès configurées et appliquées, il est très important de tester si le trafic est bloqué ou autorisé comme prévu.

- À partir de PC1, essayez d'obtenir un accès Telnet à n'importe quel périphérique. Cette opération doit être bloquée.
- À partir de PC1, essayez d'accéder au serveur Web/TFTP d'entreprise via le protocole HTTP. Cette opération doit être autorisée.

- À partir de PC2, essayez d'accéder au serveur Web/TFTP via le protocole HTTP. Cette opération doit être autorisée.
- À partir de PC2, essayez d'accéder au serveur Web externe via le protocole HTTP. Cette opération doit être autorisée.

En vous basant sur vos connaissances des listes de contrôle d'accès, réalisez quelques tests de connectivité supplémentaires à partir de PC1 et de PC2.

Étape 7. Vérification des résultats

Packet Tracer ne prenant pas en charge le test de l'accès TFTP, vous ne pourrez pas vérifier cette stratégie. Cependant, votre taux de réalisation doit être de 50 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 4 : configuration d'une liste de contrôle d'accès étendue numérotée pour R3

Étape 1. Définition du masque générique

La stratégie d'accès pour la moitié inférieure des adresses IP du réseau 192.168.30.0/24 requiert les conditions suivantes :

- Refus de l'accès au réseau 192.168.20.0/24
- Autorisation de l'accès vers toutes les autres destinations

La moitié supérieure des adresses IP du réseau 192.168.30.0/24 possède les restrictions suivantes :

- Autorisation de l'accès à 192.168.10.0 et à 192.168.11.0
- Refus de l'accès à 192.168.20.0
- Autorisation des accès Web et ICMP vers tous les autres emplacements

Pour définir le masque générique, réfléchissez aux bits qui doivent être testés pour que la liste de contrôle d'accès corresponde aux adresses IP 0-127 (moitié inférieure) ou 128-255 (moitié supérieure).

Rappelez-vous qu'une manière de déterminer le masque générique consiste à soustraire le masque réseau normal de 255.255.255.255. Le masque normal pour les adresses IP 0-127 et 128-255 dans le cas d'une adresse de classe C est 255.255.255.128. En utilisant la méthode par soustraction, voici le masque générique qui convient :

```
   255.255.255.255
 - 255.255.255.128
-----------------
     0. 0. 0.127
```

Étape 2. Configuration des listes de contrôle d'accès étendues sur R3

Sur R3, passez en mode de configuration globale et configurez la liste de contrôle d'accès avec le numéro de liste d'accès 130.

La première instruction empêche l'hôte 192.168.30.0/24 d'accéder à toutes les adresses du réseau 192.168.30.0/24.

```
R3(config)#access-list 130 deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255
```

La seconde instruction permet à la moitié inférieure du réseau 192.168.30.0/24 d'accéder à toutes les autres destinations.

```
R3(config)#access-list 130 permit ip 192.168.30.0 0.0.0.127 any
```

Les instructions suivantes autorisent explicitement la moitié supérieure du réseau 192.168.30.0/24 à accéder aux réseaux et aux services permis par la stratégie réseau.

```
R3(config)#access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.10.0
0.0.0.255
R3(config)# access-list 130 permit ip 192.168.30.128 0.0.0.127 192.168.11.0
0.0.0.255
R3(config)# access-list 130 permit tcp 192.168.30.128 0.0.0.127 any eq www
R3(config)# access-list 130 permit icmp 192.168.30.128 0.0.0.127 any
R3(config)# access-list 130 deny ip any any
```

Étape 3. Application de l'instruction à l'interface

Pour appliquer une liste de contrôle d'accès à une interface, passez en mode de configuration d'interface. Configurez la commande **ip access-group** *numéro-liste-accès* {**in** | **out**} pour appliquer la liste de contrôle d'accès à l'interface.

```
R3(config)#interface fa0/0
R3(config-if)#ip access-group 130 in
```

Étape 4. Vérification et test des listes de contrôle d'accès

Une fois la liste de contrôle d'accès configurée et appliquée, il est très important de tester si le trafic est bloqué ou autorisé comme prévu.

- À partir de PC3, envoyez une requête ping au serveur Web/TFTP. Cette opération doit être bloquée.
- À partir de PC3, envoyez une requête ping vers tout autre périphérique. Cette opération doit être autorisée.
- À partir de PC4, envoyez une requête ping au serveur Web/TFTP. Cette opération doit être bloquée.
- À partir de PC4, ouvrez une session Telnet vers R1 à l'adresse 192.168.10.1 ou 192.168.11.1. Cette opération doit être autorisée.
- À partir de PC4, envoyez une requête ping à PC1 et à PC2. Cette opération doit être autorisée.
- À partir de PC4, ouvrez une session Telnet vers R2 à l'adresse 10.2.2.2. Cette opération doit être bloquée.

Une fois que les tests ont donné les résultats attendus, lancez la commande d'exécution privilégiée **show access-lists** sur R3 pour vérifier que les instructions de liste de contrôle d'accès ont des correspondances.

En vous basant sur vos connaissances des listes de contrôle d'accès, réalisez d'autres tests pour vérifier que chaque instruction correspond au trafic correct.

Étape 5. Vérification des résultats

Votre taux de réalisation doit être de 75 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.

Tâche 5 : configuration d'une liste de contrôle d'accès étendue nommée

Étape 1. Configuration d'une liste de contrôle d'accès étendue nommée sur R2

Rappelez-vous que la stratégie sur R2 doit être conçue pour filtrer le trafic Internet. R2 ayant une connexion au fournisseur de services (FAI), il constitue le meilleur emplacement pour la liste de contrôle d'accès.

Configurez une liste de contrôle d'accès nommée FIREWALL sur R2 à l'aide de la commande **ip access-list extended** *nom*. Cette commande place le routeur en mode de configuration de liste de contrôle d'accès nommée. Remarquez que l'invite du routeur est différente.

```
R2(config)#ip access-list extended FIREWALL
R2(config-ext-nacl)#
```

En mode de configuration de liste de contrôle d'accès, ajoutez les instructions de filtrage du trafic décrites dans la stratégie :

- Les hôtes externes peuvent établir une session Web avec le serveur Web interne uniquement sur le port 80.
- Seules les sessions TCP établies sont autorisées en entrée.
- Les réponses ping sont autorisées via R2.

```
R2(config-ext-nacl)#permit tcp any host 192.168.20.254 eq www
R2(config-ext-nacl)#permit tcp any any established
R2(config-ext-nacl)#permit icmp any any echo-reply
R2(config-ext-nacl)#deny ip any any
```

Une fois la liste de contrôle d'accès configurée sur R2, lancez la commande **show access-lists** pour vérifier que la liste contient les instructions correctes.

Étape 2. Application de l'instruction à l'interface

Lancez la commande **ip access-group** *nom* {**in** | **out**} pour appliquer la liste de contrôle d'accès en entrée de l'interface de R2 reliée à FAI.

```
R3(config)#interface s0/1/0
R3(config-if)#ip access-group FIREWALL in
```

Étape 3. Vérification et test des listes de contrôle d'accès

Réalisez les tests suivants pour vous assurer que la liste de contrôle d'accès fonctionne comme prévu :

- À partir de Outside Host, ouvrez une page Web sur le serveur Web/TFTP interne. Cette opération doit être autorisée.
- À partir de Outside Host, envoyez une requête ping au serveur Web/TFTP interne. Cette opération doit être bloquée.
- À partir de Outside Host, envoyez une requête ping à PC1. Cette opération doit être bloquée.
- À partir de PC1, envoyez une requête ping au serveur Web à l'adresse 209.165.201.30. Cette opération doit être autorisée.
- À partir de PC1, ouvrez une page Web sur le serveur Web externe. Cette opération doit être autorisée.

Une fois que les tests ont donné les résultats attendus, lancez la commande d'exécution privilégiée **show access-lists** sur R2 pour vérifier que les instructions de liste de contrôle d'accès ont des correspondances.

En vous basant sur vos connaissances des listes de contrôle d'accès, réalisez d'autres tests pour vérifier que chaque instruction correspond au trafic correct.

Étape 4. Vérification des résultats

Votre taux de réalisation doit être de 100 %. Si ce n'est pas le cas, cliquez sur **Check Results** pour identifier les composants nécessaires qui ne sont pas complets.