Objectifs :

À l'issue de ces travaux pratiques, vous serez en mesure d'effectuer les tâches suivantes :

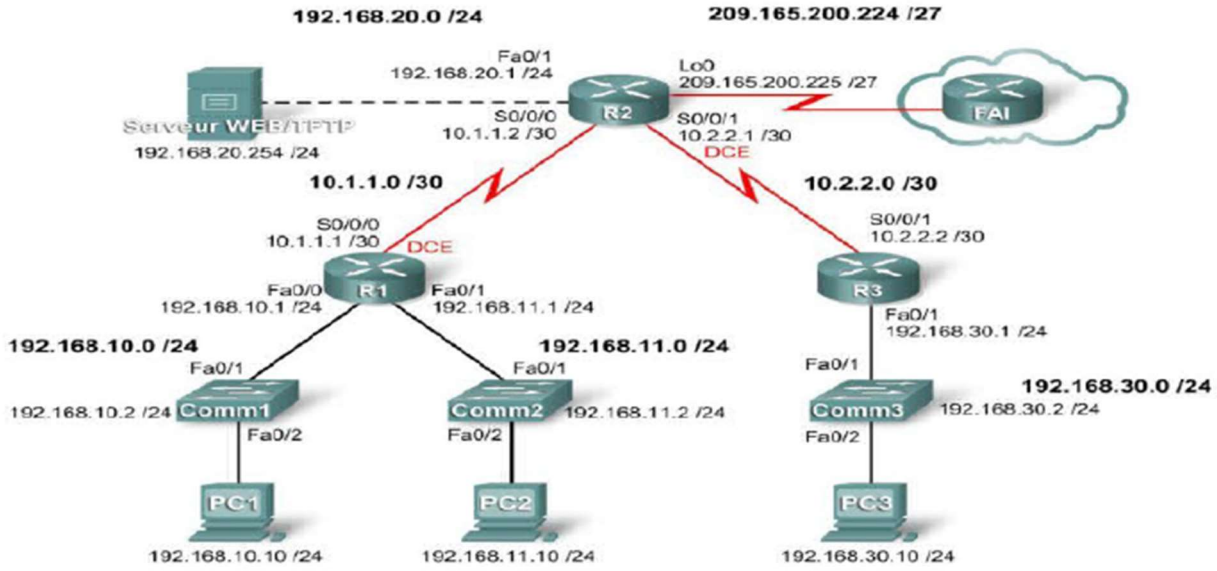
- Concevoir des listes de contrôle d'accès nommées standard et étendues
- Appliquer des listes de contrôle d'accès nommées standard et étendues
- Tester des listes de contrôle d'accès nommées standard et étendues
- Résoudre les problèmes liés aux listes de contrôle d'accès nommées standard et étendues

Scénario

Dans le cadre de ces travaux pratiques, vous apprendrez à configurer la sécurité d'un réseau de base à l'aide des listes de contrôle d'accès. Vous appliquerez des listes de contrôles d'accès standard et étendues.

Tâche 1 : Préparation du réseau

Faire la configuration de la topologie présentée ci-dessous.



Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	Fa0/0	192.168.10.1	255.255.255.0	
	Fa0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
R2	Fa0/1	192.168.20.1	255.255.255.0	
	S0/0/0	10.1.1.2	255.255.255.252	
	S0/0/1	10.2.2.1	255.255.255.252	
	Lo0	209.165.200.225	255.255.255.224	
R3	Fa0/1	192.168.30.1	255.255.255.0	
	S0/0/1	10.2.2.2	255.255.255.252	
Comm1	Vlan1	192.168.10.2	255.255.255.0	192.168.10.1
Comm2	Vlan1	192.168.11.2	255.255.255.0	192.168.11.1
Comm3	Vlan1	192.168.30.2	255.255.255.0	192.168.30.1
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
Serveur Web	Carte réseau	192.168.20.254	255.255.255.0	192.168.20.1

Tâche 2 : configuration d'une liste de contrôle d'accès standard

Dans cette tâche, vous allez configurer une liste de contrôle d'accès standard. La liste de contrôle d'accès est conçue pour bloquer le trafic provenant du réseau 192.168.11.0/24, et ce afin de l'empêcher d'accéder à des réseaux locaux sur R3. Cette liste est appliquée en entrée, sur l'interface série de R3. Avant de configurer et d'appliquer cette liste, veillez à vérifier la connectivité depuis PC1 (ou l'interface Fa0/1 sur R1) vers PC3 (ou l'interfaceFa0/1 sur R3). Les tests de connectivité doivent aboutir avant d'appliquer cette liste.

Étape 1 : création de la liste de contrôle d'accès sur le routeur R3

En mode de configuration globale, créez une liste de contrôle d'accès standard nommée

STND-1

R3(config)# ***ip access-list standard STND-1***

En mode de configuration de liste de contrôle d'accès standard, ajoutez une instruction chargée de refuser tous les paquets dont l'adresse source est 192.168.11.0/24 et d'ajouter un message dans la console pour chaque paquet correspondant.

R3(config-std-nacl)# ***deny 192.168.11.0 0.0.0.255 log***

Autorisez le reste du trafic.

R3(config-std-nacl)# ***permit any***

Étape 2 : application de la liste de contrôle d'accès

Appliquez la liste de contrôle d'accès **STND-1** pour filtrer les paquets entrant dans R3, par le biais de l'interface série 0/0/1.

R3(config)# **interface serial 0/0/1**

R3(config-if)# **ip access-group STND-1 in**

R3(config-if)# **end**

R3#**copy run start**

Étape 3 : test de la liste de contrôle d'accès

Vérifiez la liste de contrôle d'accès en envoyant une requête ping vers le PC3 à partir du PC2. La liste de contrôle d'accès étant conçue pour bloquer le trafic dont l'adresse source fait partie du réseau 192.168.11.0/24, le PC2 (192.168.11.10) ne peut normalement pas envoyer de requêtes ping vers le PC3.En mode d'exécution privilégié sur R3, lancez la commande

show access-lists

Une sortie similaire à la suivante s'affiche. Chaque ligne d'une liste de contrôle d'accès possède un compteur associé, qui affiche le nombre de paquets correspondants à la règle.

Standard IP access list STND-110 deny 192.168.11.0, wildcard bits 0.0.0.255 log (5 matches)20 permit any (25 matches)

Tâche 3 : configuration d'une liste de contrôle d'accès étendue

Une autre stratégie mise en place pour ce réseau indique que les périphériques du réseau local 192.168.10.0/24 ne peuvent accéder qu'aux réseaux internes. Les ordinateurs de ce réseau local ne sont pas autorisés à accéder à Internet. Par conséquent, ces utilisateurs ne doivent pas pouvoir accéder à l'adresse IP 209.165.200.225. Cette exigence s'appliquant à la source et à la destination, il est nécessaire d'utiliser une liste de contrôle d'accès étendue. Cette tâche consiste à configurer une liste de contrôle d'accès étendue sur R1, qui sera chargée d'empêcher le trafic en provenance d'un périphérique du réseau 192.168.10.0 /24 d'accéder à l'hôte 209.165.200.225. Cette liste de contrôle d'accès sera appliquée en sortie de l'interface série 0/0/0 de R1. Pour appliquer de façon optimale des listes de contrôle d'accès étendues, il est conseillé de les placer aussi près que possible de la source. Avant de commencer, vérifiez que vous pouvez envoyer une requête

ping vers 209.165.200.225 depuis le PC1.

Étape 1 : configuration d'une liste de contrôle d'accès étendue nommée

En mode de configuration globale, créez une liste de contrôle d'accès étendue nommée

EXTEND-1

R1(config)# i***p access-list extended EXTEND-1***

Vous remarquerez que l'invite du routeur change pour indiquer que le routeur est à présent en mode de configuration de liste de contrôle d'accès étendue. À partir de cette invite, ajoutez les instructions nécessaires pour bloquer le trafic provenant du réseau 192.168.10.0 /24 à destination de l'hôte. Utilisez le mot clé **host** lors de la définition de la destination. R1

(config-ext-nacl)# ***deny ip 192.168.10.0 0.0.0.255 host 209.165.200.225***

(config-ext-nacl)# ***permit ip any any***

Étape 2 : application de la liste de contrôle d'accès

Les listes de contrôle d'accès étendues sont souvent placées près de la source. La liste

EXTEND-1 sera placée sur l'interface série et filtrera le trafic sortant.R1(config)#

interface serial 0/0/0

R1(config-if)# **ip access-group EXTEND-1 out log**

R1(config-if)# **end**

R1# **copy run start**

Étape 3 : test de la liste de contrôle d'accès

Vous pouvez effectuer une vérification approfondie en entrant la commande

show ip access-list sur R1 après l'envoi de la requête ping.