ACTIVITE 4
Configurer des ACLs

L'objectif de cette activité est de configurer une liste d'accès (ACL) sur l'interface d'un routeur.

1 – Configurer et appliquer une ACL standard nommée

Utilisez le fichier "Act 4.1 - Configurer des ACL standards.pkt" pour la suite de l'activité.

Votre mission

Vous devez 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. PC1 (Web manager) et Serveur Web doivent accéder au serveur de fichiers. Tout autre trafic vers le serveur de fichiers doit être refusé.

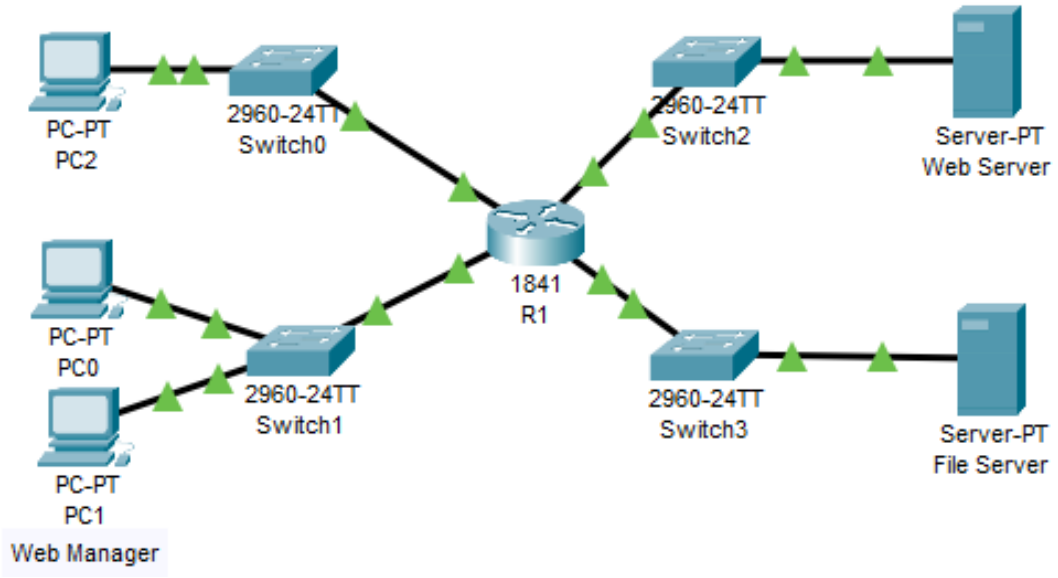


Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	E0/0/0	192.168.10.1	255.255.255.0	
	E0/1/0	192168.20,1	255.255.255.0	
	F0/0	192.168.100.1	255.255.255.0	
	F0/1	192.168.200.1	255.255.255.0	
Serveur de fichiers	Carte d'interface réseau (NIC)	192.168.200.100	255.255.255.0	192.168.200.1
Serveur web	Carte d'interface réseau (NIC)	192.168.100.100	255.255.255.0	192.168.100.1
PC0	Carte d'interface réseau (NIC)	192.168.20.3	255.255.255.0	192168.20,1
PC1	Carte d'interface réseau (NIC)	192.168.20.4	255.255.255.0	192168.20,1
PC2	Carte d'interface réseau (NIC)	192.168.10.3	255.255.255.0	192.168.10.1

☞ 1 – Vérification de la connectivité : PC0, PC1 et PC2 doivent être en mesure d'envoyer un ping au serveur Web et au serveur de fichiers.

1 - Configurer une ACL standard nommée

✍ 2 – Affectez les règles du routeur R1 à la bonne interface.

Routeur R1								
Règles	**Eth 0/0/0**		**Eth 0/1/0**		**Fa 0/0**		**Fa 0/1**	
	in	**out**	**in**	**out**	**in**	**out**	**in**	**out**
PC1 (Web Manager) peut accéder au Serveur de fichier								**X**
Tout autre trafic vers le serveur de fichiers doit être refusé								**X**
Web Serveur peut accéder au Serveur de fichier								**X**

✍ 3 – En fonction du tableau de la question 2, ordonnez les règles.

PC1 (Web Manager) peut accéder au Serveur de fichier
Web Serveur peut accéder au Serveur de fichier
Tout autre trafic vers le serveur de fichiers doit être refusé

✍ 4 – Configurez l'ACL sur le routeur R1. Vous utiliserez l'onglet CLI du routeur et vous nommerez votre liste : **R1_SERVEUR_FICHIERS**

Commandes CISCO :

```
R1(config)#ip access-list standard R1_SERVEUR_FICHIERS
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
```

✍ 5 – 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. Copiez / collez le résultat ici :

```
R1# show access-lists
Standard IP access list R1_SERVEUR_FICHIERS
10 permit host 192.168.20.4
20 permit host 192.168.100.100
30 deny any
```

✍ 6 – Appliquez l'ACL sur la bonne interface du routeur.

Commandes CISCO :

```
R1(config)#interface Fa0/1
R1(config-if)#ip access-group R1_SERVEUR_FICHIERS out
```

☞ 7 – Sauvegardez la configuration.

☞ 8 – Vérifiez avec la commande **show run** ou **show ip interface fastethernet 0/1** que la liste de contrôle d'accès est appliquée correctement à l'interface.

2 - Vérifiez que l'ACL fonctionne correctement.

☞ 9 – Testez l'ensemble des règles sortantes pour l'interface Fa0/1 du routeur R1.

- Depuis PC0, faire un ping vers le Serveur de Fichier. Le ping ne doit pas aboutir. Exécuter la commande **show access-lists** pour voir le nombre de paquets qui correspondent à chaque déclaration. Le nombre en fin de ligne vous indique le nombre de fois que la règle a été validée.

- Depuis PC1 (Web Manager), faire un ping vers le Serveur de Fichier. Le ping doit aboutir. Exécuter la commande **show access-lists** pour voir le nombre de paquets qui correspondent à chaque déclaration.

- Depuis PC2, faire un ping vers le Serveur de Fichier. Le ping ne doit pas aboutir. Exécuter la commande **show access-lists** pour voir le nombre de paquets qui correspondent à chaque déclaration.

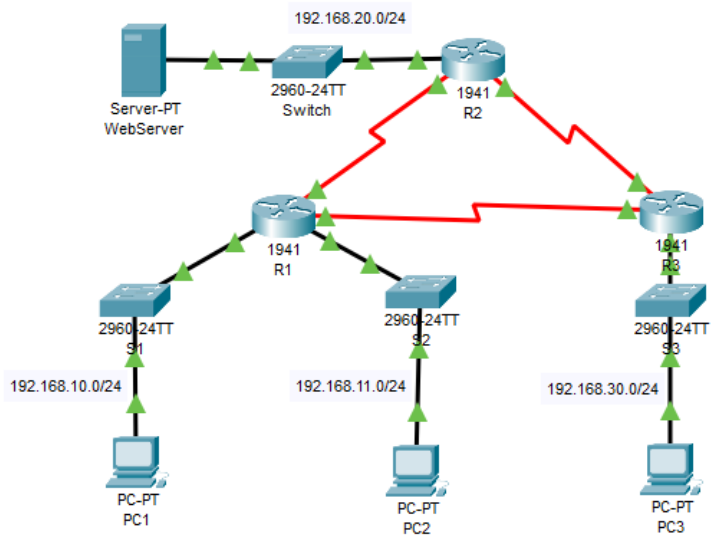
- Depuis Web Server, faire un ping vers le Serveur de Fichier. Le ping doit aboutir. Exécuter la commande **show access-lists** pour voir le nombre de paquets qui correspondent à chaque déclaration.

2 - Configurer les ACLs IPv4 standard numérotées

Utilisez le fichier "Act 4.2 - Configurer des ACL standards.pkt" pour la suite de l'activité.

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	
	G0/1	192.168.11.1	255.255.255.0	
	S0/0/0	10.1.1.1	255.255.255.252	
	S0/0/1	10.3.3.1	255.255.255.252	
R2	G0/0	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	
R3	G0/0	192.168.30.1	255.255.255.0	
	S0/0/0	10.3.3.2	255.255.255.252	
	S0/0/1	10.2.2.2	255.255.255.252	
PC1	Carte réseau (NIC)	192.168.10.10	255.255.255.0	192.168.10.1
PC2	Carte réseau (NIC)	192.168.11.10	255.255.255.0	192.168.11.1
PC3	Carte réseau (NIC)	192.168.30.10	255.255.255.0	192.168.30.1
ServeurWeb	Carte réseau (NIC)	192.168.20.254	255.255.255.0	192.168.20.1



Les routeurs sont déjà configurés, y compris le routage d'adresses IP et de protocole EIGRP (Enhanced Interior Gateway Routing Protocol).

☞ 10 – 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.

Votre mission

Votre entreprise souhaite mettre en place cette politique réseau :

- Le réseau 192.168.11.0/24 n'est pas autorisé à accéder au serveur Web du réseau 192.168.20.0/24.
- Le réseau 192.168.10.0/24 n'est pas autorisé à communiquer avec le réseau 192.168.30.0/24.
- Tout autre accès est autorisé.

✍ 11 – Attribuez les règles aux routeurs concernés.

Règles	Routeur R1	Routeur R2	Routeur R3
Le réseau 192.168.11.0/24 n'est pas autorisé à accéder au serveur Web du réseau 192.168.20.0/24.		X	
Le réseau 192.168.10.0/24 n'est pas autorisé à communiquer avec le réseau 192.168.30.0/24.			X
Tout autre accès est autorisé.		X	X

✍ 12 – En fonction de vos choix à la question 11, affectez les règles du routeur R2 à la bonne interface.

Routeur R2								
Règles	S0/0/0		S0/0/1		G0/0		G0/1	
	in	out	in	out	in	out	in	out
Le réseau 192.168.11.0/24 n'est pas autorisé à accéder au serveur Web du réseau 192.168.20.0/24.						X		
Tout autre accès est autorisé.						X		

✍ 13 – En fonction du tableau de la question 12, ordonnez les règles.

Règle 1 : Le réseau 192.168.11.0/24 n'est pas autorisé à accéder au serveur Web du réseau 192.168.20.0/24.
Règle 2 : Tout autre accès est autorisé.

✍ 14 – Configurez l'ACL sur le routeur R2. Vous utiliserez le numéro 1 votre liste sur R2.

Commandes CISCO :

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

Par défaut, une liste d'accès refuse tout le trafic qui ne correspond à aucune règle. Pour autoriser tout autre trafic la dernière ligne de l'ACL est très importante.

✍ 15 – Utilisez la commande **show access-lists** pour vérifier le contenu de la liste d'accès avant de l'appliquer à une interface. Copiez / collez le résultat ici :

```
R2#show access-lists
Standard IP access list 1
        10 deny 192.168.11.0 0.0.0.255
        20 permit any
```

✍ 16 – Appliquez l'ACL sur la bonne interface du routeur R2.

Commandes CISCO :

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

☞ 17 – Sauvegardez la configuration.

☞ 18 – Vérifiez avec la commande **show run** ou **show ip interface G0/0** que la liste de contrôle d'accès est appliquée correctement à l'interface.

✍ 19 – En fonction de vos choix à la question 11, affectez les règles du routeur R3 à la bonne interface.

Routeur R3								
Règles	**S0/0/0**		**S0/0/1**		**G0/0**		**G0/1**	
	in	**out**	**in**	**out**	**in**	**out**	**in**	**out**
Le réseau 192.168.10.0/24 n'est pas autorisé à communiquer avec le réseau 192.168.30.0/24.						**X**		
Tout autre accès est autorisé.						**X**		

✍ 20 – En fonction du tableau de la question 19, ordonnez les règles.

Le réseau 192.168.10.0/24 n'est pas autorisé à communiquer avec le réseau 192.168.30.0/24.
Tout autre accès est autorisé.

✍ 21 – Configurez l'ACL sur le routeur R3. Vous utiliserez le numéro 1 votre liste sur R3.

Commandes CISCO :

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

✍ 22 – Utilisez la commande **show access-lists** pour vérifier le contenu de la liste d'accès avant de l'appliquer à une interface. Copiez / collez le résultat ici :

```
R3# show access-lists
Standard IP access list 1
        10 deny 192.168.10.0 0.0.0.255
        20 permit any
```

✍ 23 – Appliquez l'ACL sur la bonne interface du routeur R3.

Commandes CISCO :

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

☞ 24 – Vérifiez avec la commande **show run** ou **show ip interface G0/0** que la liste de contrôle d'accès est appliquée correctement à l'interface.

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

☞ 25 – Avec les deux listes de contrôle d'accès en place, le trafic réseau est limité en fonction des stratégies détaillées dans la politique réseau de l'entreprise. 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.

✍ 26 – Exécutez à nouveau la commande **show access-lists** sur les routeurs R2 et R3 . Vous devriez voir une sortie qui indique le nombre de paquets qui correspondent à chaque ligne de la liste d'accès.

Remarque : Le nombre de correspondances affichées pour vos routeurs est lié au nombre de pings envoyés et reçus.

Copiez / collez le résultat ici pour le routeur R2 :

```
R2#show access-lists
Standard IP access list 1
        10 deny 192.168.11.0 0.0.255 (4 match (s))
        20 permit any (8 match(es))
```

Copiez / collez le résultat ici pour le routeur R3 :

```
R3#show access-lists
Standard IP access list 1
        10 deny 192.168.10.0 0.0.0.255 (4 match(es))
        20 permit any (8 match(es))
```