Université Mohammed Premier Oujda
École Nationale des Sciences Appliquées
Département : Électronique, Télécommunications et Informatique
Filière : GI/GSEIR / Niveau : GI5/GSEIR5
Module : Sécurité des réseaux

TP3 Security :

Configuration et vérification des listes de contrôle d'accès étendues

Enseignant : Mohammed SABER

Année Universitaire : 2017/2018

Objectifs pédagogiques de TP :

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

Partie 1 : configuration de la topologie et initialisation des périphériques

- Configurez l'équipement pour qu'il corresponde à la topologie du réseau.
- Initialisez et redémarrez les routeurs et les commutateurs.

Partie 2 : configuration des périphériques et vérification de la connectivité

- Attribuez une adresse IP statique aux PC.
- Configurez les paramètres de base sur les routeurs.
- Configurez les paramètres de base sur les commutateurs.
- Configurez le routage (RIP, EIGRP, OSPF) sur R1, R2 et R3.
- Vérifiez la connectivité entre les périphériques.

Partie 3 : configuration et vérification des listes de contrôle d'accès numérotées et nommées standard

- Configurez, appliquez et vérifiez une liste de contrôle d'accès étendue numérotée.
- Configurez, appliquez et vérifiez une liste de contrôle d'accès étendue nommée.

Partie 4 : modification d'une liste de contrôle d'accès standard

- Modifiez et vérifiez une liste de contrôle d'accès étendue nommée.
- Testez la liste de contrôle d'accès.

Scénario

La sécurité réseau est un sujet important lors de la conception et de la gestion des réseaux IP. La possibilité de configurer des règles appropriées pour filtrer les paquets, sur base de politiques de sécurité définies, est une compétence importante.

Dans ces travaux pratiques, vous allez configurer le filtrage des règles pour les trois réseaux représentés par **R1**, **R2** et **R3**. La direction a établi certaines stratégies d'accès entre les LANs situés au niveau de **R1**, **R2** et **R3**, que vous devez implémenter.

Remarque : Assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre enseignant.

Ressources requises

Ressources nécessaires :

1. Trois routeurs, chacun équipé des interfaces de type Ethernet et série ;
2. Trois ordinateurs Windows 7,dont un avec un programme d'émulation de terminal (PuTTY) ;

3. Six câbles Ethernet directs (PC-A à SW1, SW1 à R1, R2 à SW2, SW2 à PC-D, R3 à SW3 et SW3 à PC-G) ;
4. Trois câbles série null-modem (R1 à R2, R1 à R3 et R3 à R2) ;
5. Trois câbles console avec connecteur RJ-45 vers DB-9 (PC-A à R1, PC-D à R2 et PC-G à R3) ;
6. Accès à l'invite de commandes des hôtes PC-A, PC-D et PC-G ;
7. Accès à la configuration TCP/IP du réseau des hôtes PC-A, PC-D et PC-G.
8. Accès à l'invite de commandes des hôtes VM sur PC-A (PC-B et PC-C), PC-D (PC-E et PC-F) et PC-G (PC-H et PC-I) ;
9. Accès à la configuration TCP/IP du réseau des hôtes VM sur PC-A (PC-B et PC-C), PC-D (PC-E et PC-F) et PC-G (PC-H et PC-I) ;
10. Trois commutateurs (Switch) ;

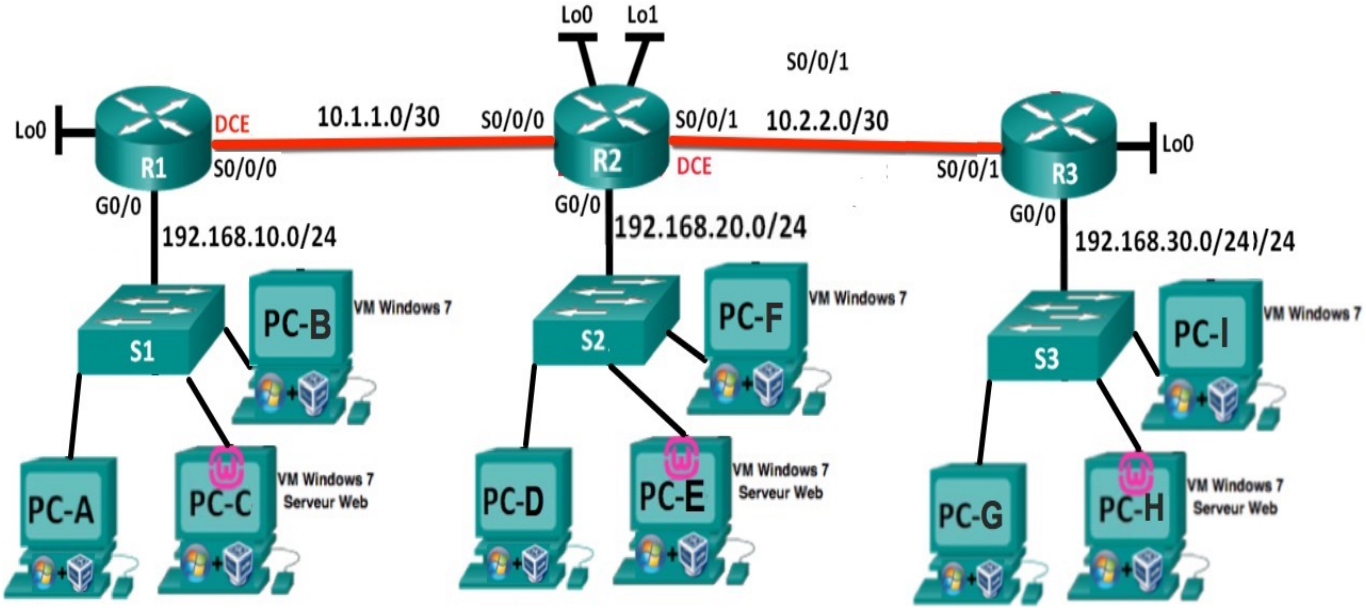
Consignes pour le TP

1. Suivez les instructions pour chaque étape.
2. Ne déplacez pas le matériel.
3. **N'utilisez pas les Clés USB sur les machines**.
4. A la fin de TP, SVP réorganiser votre table :
   - Éteindre toutes les machines.
   - Réorganiser les chaises à ces places avant de sortir.
   - MERCI d'avance.
5. **Chaque étudiant ne respect pas les consignes de TP sera sanctionné.**

Étape 1 : Préparation du réseau

Atelier de TP

L'architecture de l'atelier du scénario est la suivante :



Câblez le réseau conformément à la topologie

. Les informations pour chaque équipement pour ces travaux pratiques sont présentées sur le tableau suivant :

Périphérique	Interface	Adresse IP	Masque réseau	Passerelle
R1	G0/1 (Type Ethernet)	192.168.10.1	255.255.255.0	N/D
	Lo0 (Type loopback)	192.168.40.1	255.255.255.0	N/D
	S0/0/0 (Type Serial)	10.1.1.1	255.255.255.252	N/D
R2 (ISP)	G0/1 (Type Ethernet)	192.168.20.1	255.255.255.0	N/D
	S0/0/0 (Type Serial)	10.1.1.2	255.255.255.252	N/D
	S0/0/1 (Type Serial)	10.2.2.2	255.255.255.252	N/D
	Lo0 (Type loopback)	209.165.200.225	255.255.255.224	N/D
	Lo1 (Type loopback)	209.165.201.1	255.255.255.224	N/D
R3	G0/1 (Type Ethernet)	192.168.30.1	255.255.255.0	N/D
	S0/0/1 (Type Serial)	10.2.2.1	255.255.255.252	N/D
	Lo0 (Type loopback)	192.168.50.1	255.255.255.0	N/D
PC-A	N/D	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	N/D	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	N/D	192.168.10.4	255.255.255.0	192.168.10.1

PC-D	N/D	192.168.20.2	255.255.255.0	192.168.20.1
PC-E	N/D	192.168.20.3	255.255.255.0	192.168.20.1
PC-F	N/D	192.168.20.4	255.255.255.0	192.168.20.1
PC-G	N/D	192.168.30.2	255.255.255.0	192.168.30.1
PC-H	N/D	192.168.30.3	255.255.255.0	192.168.30.1
PC-I	N/D	192.168.30.4	255.255.255.0	192.168.30.1

Étape 2 : Installation, suppression et rechargement des routeurs

Tâche 1 : Connexion des périphériques

Connectez les périphériques de réseau similaire à celui de la topologie de l'atelier.

Tâche 2 : suppression des configurations existantes sur les routeurs

Il est nécessaire de commencer avec un routeur non configuré. L'utilisation d'un routeur comportant déjà une configuration peut produire des résultats imprévisibles. Les étapes suivantes permettent de préparer le routeur avant d'effectuer les travaux pratiques pour que les options de configuration précédentes ne créent pas d'interférence.

1. Passez en mode d'exécution privilégié.
2. **Effacement de la configuration :** Pour effacer la configuration, lancez la commande `erase startup-config`. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment effacer la configuration actuellement enregistrée en mémoire NVRAM, appuyez sur **Entrée**.
3. **Rechargement de la configuration :** Au retour de l'invite, lancez la commande ***reload***. Si vous êtes invité à enregistrer les modifications, répondez par **no** [**Que se passerait-il si vous répondiez yes à la question**].
4. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment recharger le routeur, appuyez sur **Entrée**. Dès que le routeur a terminé l'amorçage, choisissez de ne pas utiliser la fonction **AutoInstall**.
5. Répétez les questions 1 à 4 sur le routeur R2 ?
6. Répétez les questions 1 à 4 sur le routeur R3 ?

Étape 2 : Configuration basique des routeurs Cisco

Tâche 1 : Configuration de base des routeurs

1. Configurez le nom d'hôte du routeur 1 en tant que **R1**.
2. Configurez le nom d'hôte du routeur 2 en tant que **R2**.
3. Configurez le nom d'hôte du routeur 3 en tant que **R3**.
4. Attribuez "**ensao**" au mot de passe de mode d'exécution privilégié sur les routeurs.

5. Attribuez "**ensao**" au mot de passe de console sur les routeurs.
6. Attribuez "**ensao**" au mot de passe vty sur les routeurs.
7. Affichez la configuration à l'aide de la commande `show running-config`.
8. Vérifier les mots de passe sont en clair sur les routeurs.
9. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**" sur les deux routeurs.

Tâche 2 : Désactivation des messages débogage non sollicités

1. Configurez les routeurs de sorte que les messages de console n'interfèrent pas avec l'entrée des commandes. Ceci est utile lorsque vous quittez le mode de configuration, car vous retournez à l'invite de commandes et l'option évite alors que des messages s'affichent dans la ligne de commande `logging synchronous` en **mode line** soit **console** soit **terminal virtuel VTY**.
2. Configurez le routeur de sorte que pas de délai d'attente, dans la ligne de commande `exec-timeout 0 0` en **mode line** soit **console** soit **terminal virtuel VTY**.
3. Désactivez la recherche DNS avec la commande `no ip domain-lookup`.
4. Sauvegardez la configuration actuelle `running-config` dans la configuration de démarrage `startup-config` sur les deux routeurs.

Tâche 3 : Configuration des interfaces de R1

1. En mode de configuration d'interface, configurez l'adresse IP pour l'interface série **S0/0/0** sur **R1** vers **R2**. Reportez-vous à la table Synthèse des interfaces de routeur.
2. Affectez la description suivante "**WAN link to R2**" pour cette interface.
3. Vérifiez, est ce que l'interface série du **R1** c'est elle l'interface DCE ? **Remarque :** Le type de câble (**DCE** ou **DTE**) est gravé à chaque extrémité du **câble série Null**. En cas de doute, entrez la commande ***clock rate*** sur les interfaces série des deux routeurs. La commande est ignorée sur le routeur auquel le **DTE** est connecté.
4. Si l'interface série de **R1** est DCE, configurez la fréquence d'horloge (**128000**).
5. Activez l'interface série.
6. En mode de configuration d'interface, configurez l'adresse IP pour l'interface de type Ethernet **G0/0** sur **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
7. Affectez la description suivante "**LAN link to Network10.0**" pour cette interface.
8. Activez l'interface de type Ethernet.
9. En mode de configuration d'interface, configurez l'adresse IP pour l'interface Loopback **Lo0** sur **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
10. Affectez la description suivante "**LAN link to Network40.0**" pour cette interface.
11. Activez l'interface Loopback.
12. Affichez la table de routage.
13. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**".

Tâche 4 : Configuration des interfaces de R2

1. En mode de configuration d'interface, configurez l'adresse IP pour l'interface série **S0/0/0** sur **R2** vers **R1**. Reportez-vous à la table Synthèse des interfaces de routeur.
2. Affectez la description suivante "**WAN link to R1**" pour cette interface.
3. Vérifiez, est ce que l'interface série du **R2** c'est elle l'interface DCE ? **Remarque :** Le type de câble (**DCE** ou **DTE**) est gravé à chaque extrémité du **câble série Null**. En cas de doute, entrez la commande ***clock rate*** sur les interfaces série des deux routeurs. La commande est ignorée sur le routeur auquel le **DTE** est connecté.
4. Si l'interface série de R2 est DCE, configurez la fréquence d'horloge (**128000**).
5. Activez l'interface série.
6. En mode de configuration d'interface, configurez l'adresse IP pour l'interface série **S0/0/1** sur **R2** vers **R3**. Reportez-vous à la table Synthèse des interfaces de routeur.
7. Affectez la description suivante "**WAN link to R3**" pour cette interface.
8. Vérifiez, est ce que l'interface série du R2 c'est elle l'interface DCE ? **Remarque :** Le type de câble (**DCE** ou **DTE**) est gravé à chaque extrémité du **câble série Null**. En cas de doute, entrez la commande ***clock rate*** sur les interfaces série des deux routeurs. La commande est ignorée sur le routeur auquel le **DTE** est connecté.
9. Si l'interface série de **R2** est DCE, configurez la fréquence d'horloge (**128000**).
10. Activez l'interface série.
11. Affichez la table de routage.
12. En mode de configuration d'interface, configurez l'adresse IP pour l'interface de type Ethernet **G0/0** sur **R2**. Reportez-vous à la table Synthèse des interfaces de routeur.
13. Affectez la description suivante "**LAN link to Network20.0**" pour cette interface.
14. Activez l'interface de type Ethernet.
15. En mode de configuration d'interface, configurez l'adresse IP pour l'interface Loopback **Lo0** sur **R2**. Reportez-vous à la table Synthèse des interfaces de routeur.
16. Affectez la description suivante "**LAN link to Network-WAN1**" pour cette interface.
17. Activez l'interface Loopback.
18. En mode de configuration d'interface, configurez l'adresse IP pour l'interface Loopback **Lo1** sur **R2**. Reportez-vous à la table Synthèse des interfaces de routeur.
19. Affectez la description suivante "**LAN link to Network-WAN2**" pour cette interface.
20. Activez l'interface Loopback.
21. Affichez la table de routage.
22. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**".

Tâche 5 : Configuration des interfaces de R3

1. En mode de configuration d'interface, configurez l'adresse IP pour l'interface série **S0/0/1** sur **R3** vers **R2**. Reportez-vous à la table Synthèse des interfaces de routeur.
2. Affectez la description suivante "**WAN link to R2**" pour cette interface.

3. Vérifiez, est ce que l'interface série du **R3** c'est elle l'interface DCE ? **Remarque :** Le type de câble (**DCE** ou **DTE**) est gravé à chaque extrémité du **câble série Null**. En cas de doute, entrez la commande ***clock rate*** sur les interfaces série des deux routeurs. La commande est ignorée sur le routeur auquel le **DTE** est connecté.
4. Si l'interface série de **R3** est DCE, configurez la fréquence d'horloge (**128kbps**).
5. Activez l'interface série.
6. Affichez la table de routage.
7. En mode de configuration d'interface, configurez l'adresse IP pour l'interface de type Ethernet **G0/1** sur **R3**. Reportez-vous à la table Synthèse des interfaces de routeur.
8. Affectez la description suivante "**LAN link to Network30.0**" pour cette interface.
9. Activez l'interface de type Ethernet.
10. En mode de configuration d'interface, configurez l'adresse IP pour l'interface Loopback **Lo0** sur **R3**. Reportez-vous à la table Synthèse des interfaces de routeur.
11. Affectez la description suivante "**LAN link to Network50.0**" pour cette interface.
12. Activez l'interface Loopback.
13. Affichez la table de routage.
14. Sauvegardez la configuration actuelle "**running-config**" dans la configuration de démarrage "**startup-config**".

Tâche 6 : Configuration de routage sur les routeurs

1. Pour configurer le routage sur les trois routeurs. Vous pouvez utiliser le routage dynamique à l'aide les protocoles de routage (RIP, EIGRP où OSPF).

   Rappel OSPF :
   - Pour activer le protocole **OSPF**, entrez la commande `router ospf process-ID` en mode de configuration globale.
   - Ajouter les routes par la commande suivante : `network` est : `network Adresse-IP-Sous-Réseau masque-générique area area-id`.

   Remarque : Considérez un masque générique comme l'inverse d'un masque de sous-réseau. L'inverse du masque de sous-réseau `255.255.255.252` est `0.0.0.3`. Pour calculer l'inverse du masque de sous-réseau, soustrayez le masque de sous-réseau de `255.255.255.255` :

   $$255.255.255.255 - 255.255.255.252 = 0.0.0.3 \quad (1)$$

2. Après avoir configuré le routage sur **R1**, **R2** et **R3**, vérifiez que tous les routeurs ont des tables de routage complètes indiquant tous les réseaux. Dépannez si ce n'est pas le cas.

Tâche 7 : Configuration des interfaces Ethernet des hosts

Configurez les interfaces Ethernet de PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I à l'aide des adresses IP et des passerelles par défaut indiquées dans le tableau sous le diagramme de la topologie.

Tâche 8 : Vérifiez la connectivité entre les périphériques

Remarque : il est très important de vérifier si la connectivité fonctionne avant de configurer et d'appliquer des listes d'accès ! Veillez à vous assurer que votre réseau fonctionne correctement avant de commencer à filtrer le trafic.

1. A partir de **PC-A**, envoyez une requête `ping` vers tous les hosts **PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I** et vers toutes les interfaces sur les routeurs **R1**, **R2** et **R3**. Les requêtes `ping` ont-elles abouti ?
2. A partir de **PC-D**, envoyez une requête `ping` vers tous les hosts **PC-A, PC-B, PC-C, PC-E, PC-F, PC-G, PC-H et PC-I** et vers toutes les interfaces sur les routeurs **R1**, **R2** et **R3**. Les requêtes `ping` ont-elles abouti ?
3. A partir de **PC-G**, envoyez une requête `ping` vers tous les hosts **PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-H et PC-I** et vers toutes les interfaces sur les routeurs **R1**, **R2** et **R3**. Les requêtes `ping` ont-elles abouti ?
4. A partir de **R1**, envoyez une requête `ping` vers tous les hosts **PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I** et vers toutes les interfaces sur les routeurs **R2** et **R3**. Les requêtes `ping` ont-elles abouti ?
5. A partir de **R2**, envoyez une requête `ping` vers tous les hosts **PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I** et vers toutes les interfaces sur les routeurs **R1** et **R3**. Les requêtes `ping` ont-elles abouti ?
6. A partir de **R3**, envoyez une requête `ping` vers tous les hosts **PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I** et vers toutes les interfaces sur les routeurs **R1** et **R2**. Les requêtes `ping` ont-elles abouti ?

Étape 3 : Activation des services SSH et Telnet sur les routeurs et les services WEB sur les hosts PC-C, PC-E, PC-H

Tâche 1 : Activation et test de la connectivité de service WEB sur les hosts PC-C, PC-E, PC-H

1. Démarrer les serveurs web dans les réseaux. (Démarrer à partir l'application WampServer).
2. Ouvrez un navigateur Web sur les machines **PC-A**, **PC-D**, **PC-A** et accédez à `http://adresse-IP-PC-C`. Les requêtes `WEB` ont-elles abouti ?
3. Ouvrez un navigateur Web sur les machines **PC-A**, **PC-D**, **PC-A** et accédez à `http://adresse-IP-PC-E`. Les requêtes `WEB` ont-elles abouti ?
4. Ouvrez un navigateur Web sur les machines **PC-A**, **PC-D**, **PC-A** et accédez à `http://adresse-IP-PC-H`. Les requêtes `WEB` ont-elles abouti ?

Tâche 2 : Activation de service SSH ou Telnet sur les routeurs

Remarque : l'activation de service **WEB** sur un routeur, a pour objectif de d'ouvrir des sessions à distance.

Pour cela, tapez les commandes suivantes :

- **R(config)#** `ip domain-name ensao.ma`
- **R(config)#** `crypto key generate rsa` **modulus** `1024`

- **R(config)**# `line vty 0 4`
- **R(config-line)**# `login local`
- **R(config-line)**# `transport input ssh`

1. Activez le service SSH sur R1.
2. Activez le service SSH sur R2.
3. Activez le service SSH sur R3.

Tâche 3 : Test de la connectivité SSH ou Telnet sur les routeurs

1. A partir de n'importe quelle machines **PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I**, envoyez une requête `SSH/` ou `telnet` vers les interfaces du routeurs **R1**. Les requêtes `SSH/` ou `telnet` ont-elles aboutis ?
2. A partir de n'importe quelle machines **PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I**, envoyez une requête `SSH/` ou `telnet` vers les interfaces du routeurs **R2**. Les requêtes `SSH/` ou `telnet` ont-elles aboutis ?
3. A partir de n'importe quelle machines **PC-A, PC-B, PC-C, PC-D, PC-E, PC-F, PC-G, PC-H et PC-I**, envoyez une requête `SSH/` ou `telnet` vers les interfaces du routeurs **R3**. Les requêtes `SSH/` ou `telnet` ont-elles aboutis ?

Étape 4 : Configuration et vérification des listes de contrôle d'accès étendues numérotées

Les listes de contrôle d'accès étendues permettent de filtrer le trafic de plusieurs façons. Les listes de contrôle d'accès étendues permettent de filtrer sur base des adresses IP sources, des ports sources, des adresses IP de destination, des ports de destination, ainsi que sur différents protocoles et services.

Les stratégies de sécurité sont les suivantes :

Stratégie 1 : Stratégie sur les services **WEB** : Pour les hosts du réseau **192.168.10.0/24**.
- Autoriser la machine **PC-A** de communiquer via le service Web vers le réseau **192.168.20.0/24** et non les autres machines.
- Autoriser toutes les machines de ce réseau de communiquer via le service Web vers le réseau **192.168.30.0/24** et non la machine **PC-A**.
- Le reste du traffic est refusé.

Stratégie 2 : Stratégie sur les services **SSH/TELNET** : Pour les hosts du réseau **192.168.20.0/24**.
- Autoriser la machine **PC-D** de communiquer via les services **SSH/TELNET** vers le routeur **R2** et non les autres machines.
- Autoriser toutes les machines de ce réseau de communiquer via les services **SSH/TELNET** vers les routeurs **R1** et **R3** et non la machine **PC-D**.
- Le reste du traffic est refusé.

Stratégie 3 : Stratégie sur les services **PING** : Pour les hosts du réseau **192.168.30.0/24**.
- Autoriser la machine **PC-H** de communiquer via les services **PING** vers le réseau **192.168.40.0/** et non les autres machines.
- Autoriser toutes les machines de ce réseau de communiquer via les services **PING** vers les machines des réseaux **209.165.200.224/27** et **209.165.201.0/27SSH/TELNET** des routeurs **R1** et **R3** et non la machine **PC-H**.
- Le reste du traffic est refusé.

Stratégie 4 : Stratégie sur les services **PING** :

- Autoriser la machine **PC-B** d'envoyer un `echo` vers la machine **PC-I** non vers les autres machines de réseau.
- Autoriser la machine **PC-I** de répondre à un `echo-reply` vers la machine **PC-B** non vers les autres machines de réseau.
- Le reste du traffic est refusé.

Stratégie 5 : Stratégie sur les communications :

- Autoriser les utilisateurs du réseau **192.168.10.0/24** à accéder au réseau **192.168.30.0/24**.
- Le reste du traffic est refusé.

Sur base des stratégies de sécurité mentionnées ci-dessus, vous aurez besoin au minimum de deux listes de contrôle d'accès pour satisfaire aux stratégies de sécurité. Il est conseillé de placer les listes de contrôle d'accès étendues le plus près possible de la source. Nous suivre cette pratique dans le cadre de ces stratégies.

Tâche 1 : Configurez une liste de contrôle d'accès étendue numérotée (ACL 100) pour la stratégie de sécurité 1

1. Sur quel routeur sera crée la liste de contrôle d'accès ACL ?
2. Quelles sont les plages pour les listes de contrôle d'accès étendues ?
3. Configurez la liste de contrôle d'accès pour la **stratégie 1**. Utilisez **100** comme numéro de liste de contrôle d'accès.
4. A quelle interface la liste de contrôle d'accès ACL **100** doit-elle être appliquée ?
5. Dans quelle direction la liste de contrôle d'accès ACL **100** doit-elle être appliquée ?

Tâche 2 : Vérification de la liste de contrôle d'accès ACL 100

L'utilisation de diverses commandes `show` peut vous aider à vérifier la syntaxe et l'emplacement de vos listes de contrôle d'accès sur votre routeur.

1. Vérifiez une liste de contrôle d'accès numérotée. (**Utilisation** : `show access-lists`).
2. Pour afficher la liste d'accès N dans son intégralité avec toutes les listes de contrôle d'accès, quelle commande utiliseriez-vous ? (**Utilisation** : `show access-lists N`). (**N** : Numéro de l'ACL standard crée).
3. Quelle commande utiliseriez-vous pour savoir où la liste d'accès a été appliquée et dans quelle direction ? (**Utilisation** : `show ip interface Numéro-If`).

Tâche 3 : Test de la liste de contrôle d'accès ACL 100

1. Ouvrez un navigateur Web sur **PC-A**, puis accédez au serveur WEB **PC-E**. Les requêtes `WEB` ont-elles aboutis ?
2. Ouvrez un navigateur Web sur **PC-A**, puis accédez au serveur WEB **PC-H**. Les requêtes `WEB` ont-elles aboutis ?
3. Ouvrez un navigateur Web sur **PC-B**, puis accédez au serveur WEB **PC-E**. Les requêtes `WEB` ont-elles aboutis ?
4. Ouvrez un navigateur Web sur **PC-B**, puis accédez au serveur WEB **PC-H**. Les requêtes `WEB` ont-elles aboutis ?

5. Ouvrez un navigateur Web sur **PC-I**, **PC-F**, puis accédez au serveur WEB **PC-C**. Les requêtes `WEB` ont-elles aboutis ?
6. A partir de l'invite de commande des machines **PC-A**, envoyez des requêtes `ping` aux hosts **PC-D** et **PC-G**. Pouvez-vous expliquer vos résultats ?

Tâche 4 : Configurez une liste de contrôle d'accès étendue numérotée (ACL 101) pour la stratégie de sécurité 2

1. Sur quel routeur sera crée la liste de contrôle d'accès ACL ?
2. Configurez la liste de contrôle d'accès pour la **stratégie 2**. Utilisez **101** comme numéro de liste de contrôle d'accès.
3. A quelle interface la liste de contrôle d'accès ACL **101** doit-elle être appliquée ?
4. Dans quelle direction la liste de contrôle d'accès ACL **101** doit-elle être appliquée ?

Tâche 5 : Vérification de la liste de contrôle d'accès ACL 101

L'utilisation de diverses commandes `show` peut vous aider à vérifier la syntaxe et l'emplacement de vos listes de contrôle d'accès sur votre routeur.

1. Vérifiez une liste de contrôle d'accès numérotée. (**Utilisation** : `show access-lists`).
2. Pour afficher la liste d'accès N dans son intégralité avec toutes les listes de contrôle d'accès, quelle commande utiliseriez-vous ? (**Utilisation** : `show access-lists N`). (**N** : Numéro de l'ACL standard crée).
3. Quelle commande utiliseriez-vous pour savoir où la liste d'accès a été appliquée et dans quelle direction ? (**Utilisation** : `show ip interface Numéro-If`).

Tâche 6 : Test de la liste de contrôle d'accès ACL 101

1. Établissez une connexion **SSH/TELNET** entre **PC-D** et **R2** en utilisant une adresse IP d'une interface du routeur **R2**. Les requêtes `SSH/` ou `telnet` ont-elles aboutis ?
2. Établissez une connexion **SSH/TELNET** entre **PC-D** et **R1/R3** en utilisant une adresse IP d'une interface des routeurs **R1/R3**. Les requêtes `SSH/` ou `telnet` ont-elles aboutis ?
3. Établissez une connexion **SSH/TELNET** entre **PC-F** et **R2** en utilisant une adresse IP d'une interface du routeur **R2**. Les requêtes `SSH/` ou `telnet` ont-elles aboutis ?
4. Établissez une connexion **SSH/TELNET** entre **PC-F** et **R1/R3** en utilisant une adresse IP d'une interface des routeurs **R1/R3**. Les requêtes `SSH/` ou `telnet` ont-elles aboutis ?
5. A partir de l'invite de commande des machines **PC-D**, envoyez des requêtes `ping` aux hosts **PC-A** et **PC-G**. Pouvez-vous expliquer vos résultats ?

Tâche 7 : Configurez une liste de contrôle d'accès étendue numérotée (ACL 102) pour la stratégie de sécurité 3

1. Sur quel routeur sera crée la liste de contrôle d'accès ACL ?
2. Configurez la liste de contrôle d'accès pour la **stratégie 3**. Utilisez **102** comme numéro de liste de contrôle d'accès.
3. A quelle interface la liste de contrôle d'accès ACL **102** doit-elle être appliquée ?
4. Dans quelle direction la liste de contrôle d'accès ACL **102** doit-elle être appliquée ?

Tâche 8 : Vérification de la liste de contrôle d'accès ACL 102

L'utilisation de diverses commandes `show` peut vous aider à vérifier la syntaxe et l'emplacement de vos listes de contrôle d'accès sur votre routeur.

1. Vérifiez une liste de contrôle d'accès numérotée. (**Utilisation** : `show access-lists`).
2. Pour afficher la liste d'accès N dans son intégralité avec toutes les listes de contrôle d'accès, quelle commande utiliseriez-vous ? (**Utilisation** : `show access-lists N`). (**N** : Numéro de l'ACL standard crée).
3. Quelle commande utiliseriez-vous pour savoir où la liste d'accès a été appliquée et dans quelle direction ? (**Utilisation** : `show ip interface Numéro-If`).

Tâche 9 : Test de la liste de contrôle d'accès ACL 102

1. A partir de l'invite de commande de la machine **PC-G**, envoyez des requêtes `ping` à l'interface **Lo0** du routeur **R1**. Les requêtes `ping` ont-elles aboutis ?
2. A partir de l'invite de commande de la machine **PC-G**, envoyez des requêtes `ping` aux interfaces **Loopbacks** du routeur **R2**. Les requêtes `ping` ont-elles aboutis ?
3. A partir de l'invite de commande de la machine **PC-I**, envoyez des requêtes `ping` à l'interface **Lo0** du routeur **R1**. Les requêtes `ping` ont-elles aboutis ?
4. A partir de l'invite de commande de la machine **PC-I**, envoyez des requêtes `ping` aux interfaces **Loopbacks** du routeur **R2**. Les requêtes `ping` ont-elles aboutis ?
5. Ouvrez un navigateur Web sur **PC-I**, **PC-G**, puis accédez aux serveurs WEB **PC-C** et **PC-E**. Les requêtes `WEB` ont-elles aboutis ?

Étape 5 : Configuration et vérification des listes de contrôle d'accès étendues nommées

Tâche 1 : Configurez une liste de contrôle d'accès étendue nommée

1. Sur quel(s) routeur(s) sera(ont) crée la liste de contrôle d'accès ACL ?
2. Configurez la liste de contrôle d'accès pour la **stratégie 4**. Attribuez à la liste de contrôle d'accès le nom **PING-POLICY**.
3. A quelle interface la liste de contrôle d'accès ACL **PING-POLICY** doit-elle être appliquée ?
4. Dans quelle direction la liste de contrôle d'accès ACL **PING-POLICY** doit-elle être appliquée ?

Tâche 2 : Vérification de la liste de contrôle d'accès étendue nommée

L'utilisation de diverses commandes `show` peut vous aider à vérifier la syntaxe et l'emplacement de vos listes de contrôle d'accès sur votre routeur.

1. Vérifiez une liste de contrôle d'accès nommée. (**Utilisation** : `show access-lists`).
2. Y a-t-il une différence entre cette liste de contrôle d'accès et la liste de contrôle d'accès crée dans l'étape 3 ?
3. Quelle commande utiliseriez-vous pour savoir où la liste d'accès a été appliquée et dans quelle direction ? (**Utilisation** : `show ip interface Numéro-If`).

Tâche 3 : Test de la liste de contrôle d'accès étendue nommée

1. A partir de l'invite de commande de la machine **PC-B**, envoyez des requêtes `ping` au host **PC-I**. Les requêtes `ping` ont-elles aboutis ?
2. A partir de l'invite de commande de la machine **PC-B**, envoyez des requêtes `ping` aux autres hosts. Les requêtes `ping` ont-elles aboutis ?
3. A partir de l'invite de commande de la machine **PC-I**, envoyez des requêtes `ping` au host **PC-B**. Les requêtes `ping` ont-elles aboutis ?
4. A partir de l'invite de commande de la machine **PC-I**, envoyez des requêtes `ping` aux autres hosts. Les requêtes `ping` ont-elles aboutis ?

Étape 6 : Modification d'une liste de contrôle d'accès standard

En raison des listes de contrôle d'accès appliquées sur **R1** et **R3**. La direction a décidé d'autoriser tout le trafic entre les réseaux **192.168.10.0/24** et **192.168.30.0/24**. Vous devez modifier les deux listes de contrôle d'accès sur **R1** et **R3**.

Tâche 1 : Modification de la liste de contrôle d'accès étendue ACL 100 sur R1

1. A partir du mode d'exécution privilégié sur **R1**, exécutez la commande `show access-lists`.
2. Combien y a-t-il de lignes dans cette liste d'accès ?
3. Passez en mode de configuration globale et modifiez la liste de contrôle d'accès sur **R1** (selon la modification demandée).
4. Exécutez la commande `show access-lists`. Où apparaît la nouvelle ligne que vous venez d'ajouter dans la liste de contrôle d'accès ?

Tâche 2 : Test des listes de contrôle d'accès étendues modifiées

1. A partir de **PC-A**, envoyez une requête `ping` à l'adresse IP de **PC-G**. Les requêtes `ping` ont-elles abouti ?
2. A partir de **PC-G**, envoyez une requête `ping` à l'adresse IP de **PC-A**. Les requêtes `ping` ont-elles abouti ?
3. Pourquoi les listes de contrôle d'accès ont-elles fonctionné immédiatement pour les requêtes `ping` dès que vous les avez modifiées ?

Étape 7 : Suppression des configurations sur les routeurs

Il est nécessaire de commencer avec un routeur non configuré. L'utilisation d'un routeur comportant déjà une configuration peut produire des résultats imprévisibles. Les étapes suivantes permettent de préparer le routeur avant d'effectuer les travaux pratiques pour que les options de configuration précédentes ne créent pas d'interférence.

1. Passez en mode d'exécution privilégié.
2. **Effacement de la configuration :** Pour effacer la configuration, lancez la commande ***erase startup-config***. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment effacer la configuration actuellement enregistrée en mémoire NVRAM, appuyez sur **Entrée**.

3. **Rechargement de la configuration :** Au retour de l'invite, lancez la commande ***reload***. Si vous êtes invité à enregistrer les modifications, répondez par **no** [**Que se passerait-il si vous répondiez yes à la question**].
4. Lorsque vous êtes invité à confirmer (via **[confirm]**) que vous voulez vraiment recharger le routeur, appuyez sur **Entrée**. Dès que le routeur a terminé l'amorçage, choisissez de ne pas utiliser la fonction **AutoInstall**.
5. Répétez les questions 1 à 4 sur le routeur R2 ?
6. Répétez les questions 1 à 4 sur le routeur R3 ?