Université : Ibn Khaldoun – Tiaret **Année : 2022/2023**
Faculté : Des Mathématiques & de l'Informatique **Département : Informatique**
Promotion : 2 Master_GL **Module : Sécurité Informatique**

TP : Configurations des ACL

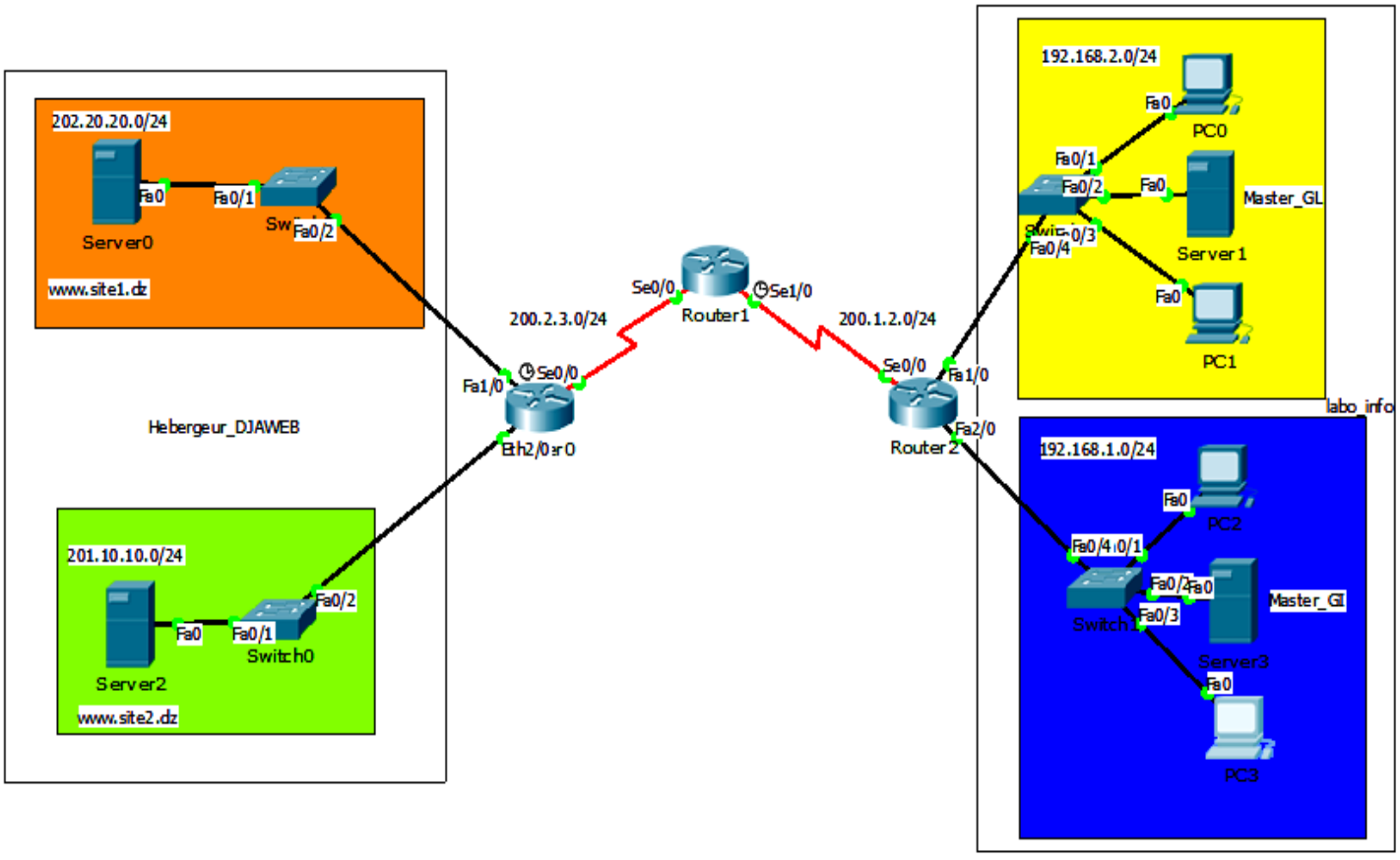
OBJECTIFS

- **Comprendre les *access-lists* standard et étendues.**
- **Mettre en œuvre plusieurs scénarios de filtrage, sur la source et/ou la destination des paquets.**

PRÉSENTATION du SCENARIO

Le schéma réseau imaginé pour effectuer ces tests est celui d'un laboratoire "Informatique" qui accéderait à différents sites, dont ceux hébergés par DJAWEB, une société qui héberge différents sites.

La maquette suivante est donc fonctionnelle en l'état, sans filtrage. Le laboratoire "Informatique" peut accéder aux 2 sites hébergés par DJAWEB.



SCENARIO 1 : ISOLATION du laboratoire Informatique

On souhaite simplement isoler **laboratoire Informatique** des autres réseaux, en permettant aux deux réseaux "Master_GL" (192.192.2.0) et "Master_GI" (192.192.1.0) de communiquer entre eux, mais pas avec le *reste du monde*.

Deux solutions peuvent être envisagées :

1. Empêcher tout trafic sortant sur Se0/0.
2. Filtrer les accès sur les deux interfaces f1/0 et f2/0

Mise en œuvre du filtrage (solution 1)

Router2(conf)# **access-list 1 deny any**

 # Application de l'access-list en sortie de s0/0

Router2(conf)# **interface s0/0**
Router2(conf-if)# **ip access-group 1 out**

Résultat obtenu / explication

Vérifions que l'accès reste possible entre Master_GL et Master_GI, mais que la communication vers un autre site n'est plus possible.

Mise en oeuvre du filtrage (solution 2)

Il nous faut d'abord annuler la règle précédente, pour éviter tout télescopage entre les deux solutions : On supprime la liste et on supprime son application sur s0/0.

Router2(conf)# **no access-list 1**
Router2(conf)# **interface s0/0/**
Router2(conf-if)# **no ip access-group 1 out**

Router2(conf)# **access-list 1 permit 192.168.1.0 0.0.0.255**
Router2(conf)# **access-list 2 permit 192.168.2.0 0.0.0.255**

Remarque importante sur le masque : Pour les *access-lists* on parle de **masque générique** : les bits positionnés (à 1) ne sont pas ceux que l'on vérifie, mais au contraire ceux que l'on ne vérifie pas. Dans les règles ci-dessus, on autorise tout le réseau 192.168.1.0 /24 ou 192.168.2.0 /24. La valeur du 4ème octet n'est pas vérifiée, mais seulement les 3 premiers octets.

 # Application de l'access-list en sortie de f1/0 et f2/0

Router2(conf)# **interface f1/0**
Router2(conf-if)# **ip access-group 1 out**
> En sortie du routeur par l'interface f1/0 qui est connectée au réseau "Master_GL", on n'autorise que les paquets qui proviennent du réseau "Master_GI"

Router2 (conf)# **interface f2/0**
Router2 (conf-if)# **ip access-group 2 out**
> En sortie du routeur par l'interface f2/0 qui est connectée au réseau "Master_GL", on n'autorise que les paquets qui proviennent du réseau "Master_GI" .

Résultat obtenu / explication

Vous devriez obtenir exactement le même résultat qu'avec la solution 1 si vous ne faites pas d'erreur. On se dispensera donc des copies d'écran. Cette fois ce sont les réponses (*du reste du monde*) qui sont filtrées, et non les envois. On peut le vérifier par une analyse des paquets.

SCENARIO 2 : ACCÈS DISTINCTIF entre les réseaux Master_GL et Master_GI

On souhaite maintenant faire une distinction entre les deux réseaux du laboratoire informatique :

- Le réseau "Master_GL" (192.192.2.0) aura accès au *reste du monde*. Et réciproquement, le réseau Master_GL (son serveur par exemple) sera accessible depuis *le reste du monde*.
- Le réseau "Master_GI" (192.168.1.0) ne pourra pas communiquer avec le *reste du monde.*

NB : La communication entre les deux réseaux "Master_GL" (192.192.2.0) et "Master_GI" (192.192.1.0) devra rester possible.

Mise en oeuvre du filtrage

Rappel : avec une *access-list* standard, on ne peut filtrer que la source. On pourrait envisager les 2 solutions, comme précédemment pour le scenario 1 :

1. Soit autoriser en sortie de s0/0 seulement ce qui provient du réseau Master_GL : Ce qui permettrait au reste du monde d'atteindre le réseau Master_GI, mais sans obtenir de réponse.

2. Soit autoriser en sortie de f0/4 uniquement ce qui provient du réseau Master_GL et ne mettre aucune règle ailleurs : Ce qui permettrait au réseau Master_GI d'envoyer des requêtes vers le reste du monde, mais il ne recevrait aucune réponse, car bloquée au retour.

Dans les deux cas, même si le filtrage est efficace, on autorise quand même des flux non souhaités, et inutiles au final puisque sans suite.

Pour isoler complètement le réseau Master_GI du reste du monde, on va utiliser deux règles :

- Une *access-list* en sortie de se0/0 qui n'autorise que les paquets "Master_GL" de sortir vers le *reste du monde*.
- Une *access-list* en entrée de se0/0 qui n'autorise que les paquets à destination de "Master_GL" de rentrer.

Comme vous l'avez sans doute deviné, la 2ème ACL ne pourra pas être une *access-list* standard puisqu'elle filtre sur la destination.
On souhaite toujours laisser les communications possibles entre les réseaux Master_GL et Master_GI.
On commence par annuler les access-lists du SCENARIO 1 qui ne sont plus nécessaires :
Router2(conf)# **no access-list 1**
Router2(conf)# **no access-list 2**
Router2(conf)# **interface f1/0**
Router2(conf-if)# **no ip access-group 1 out**
Router2(conf-if)# **exit**
Router2(conf)# **interface f2/0**
Router2(conf-if)# **no ip access-group 2 out**
Router2(conf-if)# **exit**

 # access-list standard pour s0/0 en sortie (on autorise les paquets en provenance du réseau Master_GL uniquement)

Router2(conf)# **access-list 2 permit 192.168.2.0 0.0.0.255**
access-list étendue pour s0/0 en entrée
Router1(conf)# **access-list 102 permit ip any 192.168.2.0 0.0.0.255**

Cette *access-list* nécessite des explications complémentaires :

- Une *access-list* étendue possède un n° entre 100 et 199 (ou entre 2000 et 2699). *On pourrait aussi les nommer, mais pour cette découverte, on utilisera uniquement des numéros.*
- Une *access-list* permet de définir une source et une destination, ainsi qu'un protocole, voire un n° de port.
- La source ou la destination peuvent être indiquées sous 3 formes :
  - **any** *(n'importe quelle source ou destination)*
  - <***destination***> <***masque-inversé***> *(un réseau ou une partie de réseau y compris d'ailleurs avec des bits non contigües pour le masque - ;-)*
  - **host** <***adresse-hote***> *(une seul hôte désigné par son adresse IP)*

La règle ci-dessus autorise donc tout paquet IP (que celui-ci contienne du TCP ou de l'UDP ou même de l'ICMP) à destination du réseau 192.168.2.0, et ce quelle que soit la source du paquet (*any*).

application des access-list sur s0/0
Router2(conf)# **interface s0/0**
Router2(conf-if)# **ip access-group 2 out**
Router2(conf-if)# **ip access-group 102 in**

Résultat obtenu / explication

Vérifions que l'accès reste possible entre Master_GL et Master_GI, mais que la communication vers un autre site n'est possible que depuis le réseau Master_GL.

SCENARIO 3 : ACCES RESTREINT pour le réseau Master_GL

L'accès internet pour le réseau Master_GL est "universel". Nous souhaiterions maintenant interdire l'accès à quelques sites.

Alors on souhaite simplement :

- ✓ Continuer à autoriser le réseau "Master_GL" (192.168.2.0) à avoir accès au *reste du monde*.
- ✓ Supprimer l'accès à quelques destinations, peu recommandables : www.site1.dz

NB : La communication entre les deux réseaux "Master_GL" (192.168.2.0) et "Master_GI" (192.168.1.0) devra rester possible. Même s'il est peu probable qu'on empêche cette communication, puisque le filtrage va probablement se faire sur l'interface se0/0 (interface de sortie), il est indispensable d'effectuer des tests de "non régression" quand on modifie une configuration.

Mise en œuvre du filtrage

Les nouvelles restrictions portant sur la destination, on a encore (comme c'est souvent le cas) au moins deux possibilités :

- ✓ interdire les accès sortants vers les destinations prohibées ;
- ✓ interdire les accès entrants depuis les sites prohibés.

On va choisir la solution de la raison, plutôt que la solution de la facilité : pourquoi autoriser des requêtes sortantes alors que l'on sait très bien que les réponses seront filtrées ?
Mais pour ce faire, il nous faut utiliser une *access-list* **étendue** en sortie, puisque l'on souhaite filtrer à la fois sur la source et sur la destination, alors que dans le scénario 2 on avait utilisé une **standard** en sortie.

Suppression de l'access-list précédente

Router2(conf)# **no access-list 2**
Création de l'access-list étendue 103 (il n'est pas nécessaire de modifier l'access-list 102 en entrée à priori)
Router2(conf)# **access-list 103 deny ip 192.168.2.0 0.0.0.255 202.20.20.0 0.0.0.255**
Router2(conf)# **access-list 103 permit ip 192.168.2.0 0.0.0.255 any**
Router2(conf)# **access-list 103 permit ip 192.168.1.0 0.0.0.255 any**

Association à l'interface s0/0

Router2(conf)# **interface s0/0**
Router2(conf-if)# **ip access-group 103 out**

Vérifiez que le nouveau scénario est fonctionnel :

- ✓ L'accès à **www.site2.dz** doit rester possible depuis **Master_GL**.
- ✓ L'accès à **www.site1.dz** ne soit plus être possible depuis **Master_GL.**
- ✓ Les communications entre **Master_GI** et **Master_GL** doivent toujours être possible.
- ✓ Depuis **Master_GI**, aucun accès externe n'est possible, pas plus vers **site1** et **site2.**

SCENARIO 4 : *BLACKLISTER* un PC sur WWW.site2.dz

PC0 a été repéré par le système de surveillance automatique du serveur **www.site2.dz**, ce qui va provoquer le bannissement de cet hôte fauteur de trouble, d'après son IP.

Le scenario 4 va consister à mettre en place l'*access-list*, sur Router0, qui va bannir PC0 et seulement PC0. L'interdiction se fera seulement vers le serveur www.site2.dz (on choisit de ne pas interdire tout le réseau 201.10.10.0).

Mise en oeuvre effective

Création de l'access-list étendue 104 sur Router0

Router0(conf)# **access-list 104 deny ip host 192.168.2.1 host 201.10.10.1**

Router0(conf)# **access-list 104 permit ip any any**

Association à l'interface Eth2/0

Router0(conf)# **interface Eth2/0**
Router0(conf-if)# **ip access-group 104 out**

Vérification du résultat
Par acquit de conscience, il faudrait normalement vérifier que toutes les autres communications fonctionnent (test de non régression), mais normalement cette règle étant appliquée sur un nouveau routeur, et sur une interface bien spécifique, les effets de bord sont peu probables. Vérifiez seulement que le réseau **site2** peut communiquer avec les serveurs Master_GI et Master_GL.

SCENARIO 5 : ACCES RESTRICTIF à certains SERVICES sur le réseau site2 (Server2)

Le scenario 5 autorisera uniquement l'utilisation du service HTTP :

- ✓ Le service HTTP utilise bien entendu le port TCP 80.
- ✓ Le filtrage s'effectuera en entrée, sur l'interface Se0/0 de Router0.

En effet, il est préférable de filtrer à l'entrée du routeur, pour éviter tout traitement (routage) inutile.

- ✓ Les autres accès initiés depuis l'extérieur ne sont pas acceptés : on pourra notamment tester qu'une communication FTP sur www.site2.dz échoue.

- ✓ Les autres communications doivent rester possibles, et notamment le serveur du site2 pourra continuer à accéder aux différents serveurs WEB externes et obtenir une réponse.

- ✓ Le routeur0 devra également accepter les informations concernant le protocole de routage RIP

Pour résumer, les seuls paquets entrants sur le réseau **Server2** qui seront acceptés sont :

- ✓ soit des demandes concernant les services HTTP ;
- ✓ soit des informations RIP ;
- ✓ soit des réponses à des requêtes sortantes, initiées depuis le réseau site2.

Vérifications avant mise en place du filtrage

On vérifie, avant de mettre en place ce filtrage supplémentaire, que les communications suivantes sont possibles :

- ✓ Un ping est possible depuis un **Server2** et vers un **Server2** (vers et depuis Master_GL par exemple).
- ✓ Une communication HTTP est possible depuis un **Server2** et vers www.site2.com (vers et depuis site1 par exemple).
- ✓ Une communication FTP est possible sur le **Server2**.

Mise en œuvre du filtrage

La mise en œuvre se fait donc par définition d'une *access-list* (105) et par application de cette *access-list* en **entrée de l'interface Se0/0**.

Suppression de l'access-list précédente
Router0(conf)# **no access-list 104**
Création de l'access-list étendue 105 sur Router0
Router0(conf)# **access-list 105 permit tcp any any eq www**

Association à l'interface s0/0

Router0(conf)# **interface s0/0**
Router0(conf-if)# **ip access-group 105 in**

SCENARIO 6 : AUTORISER les *PING* SORTANTS, mais REFUSER les *PING* ENTRANTS

Le scenario 6 va nous permettre de découvrir encore une autre sorte de règle, qui concerne le protocole ICMP et permet de distinguer les requêtes ICMP des réponses ICMP.

Alors chez ***Master_GL***, on souhaite se protéger des *ping*, qui sont souvent une première tentative de recherche de failles sur les réseaux ciblés par les hackers. En revanche on souhaite s'autoriser à effectuer des *ping* vers l'extérieur, sans que les réponses soient bloquées.
En résumé, on souhaite donc :

- ✓ bloquer les *ping* initiés par *le reste du monde ;*
- ✓ continuer à effectuer des *ping* sortants, et donc à recevoir les réponses *du reste du monde.*

Mise en œuvre du filtrage

Il s'agit donc de l'access-list **102** qui contient actuellement 2 règles :
Extended IP access list 102
10 permit ip any 192.168.2.0 0.0.0.255 (86 match(es))
20 permit udp any eq 520 any eq 520 (139 match(es))
Si les ping sont autorisés, c'est qu'ils sont inclus dans la 1ère règle qui concerne tout IP. Il faut donc ajouter les règles nécessaires avant la règle n° 10. On peut préciser plus ou moins la règle, en fonction ce qui est déjà paramétré, donc il n'y a pas qu'une seule possibilité. Mais il faut forcément interdire les requêtes ICMP entrantes avant la règle 10, par exemple en 5. On modifie donc la règle en insérant une nouvelle règle.

Suppression de l'access-list précédente
Router2(conf)# **no access-list 103**
Router2(conf)# **ip access-list extended 102**
Router2(conf)# **5 deny icmp any 192.168.2.0 0.0.0.255 ?**
Router2(config-ext-nacl)# **5 deny icmp any 192.168.2.0 0.0.0.255 echo**

Vérification du résultat obtenu

Il faut se souvenir que :

- ✓ Les ping vers le réseau site2 ne sont plus autorisés, puisque l'*access-list* en entrée sur ce réseau a limité les flux aux services autorisés.
- ✓ L'accès à site2 n'est pas possible pour PC0 puisqu'il est *blacklisté*.

En revanche :

- ✓ Un ping depuis PC1 vers **www.site2.com** devrait rester possible.

Enfin :

- ✓ Les ping depuis **site1.dz** et **site2.dz** n'étaient déjà plus possibles puisque la réponse ne peut pas leur parvenir du fait du filtrage sur Router2.

Donc la vérification ne peut se faire que :

- ✓ Entre PC1 et site2 pour les ping sortants qui devraient continuer à être autorisés.
- ✓ Entre Master_GL et les routeurs pour les ping sortants également (qui devraient continuer à être autorisés).
- ✓ Depuis site2 vers Master_GL, pour les ping entrants qui devraient maintenant être bloqués. (ou depuis un routeur).