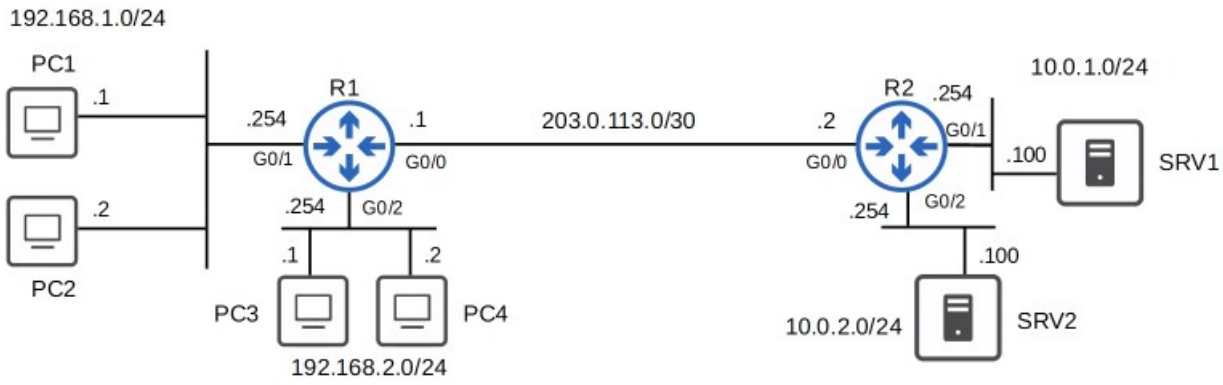
Cours 34 : Standard Access Control Lists

Dans ce cours nous allons apprendre le fonctionnement de ACL (Access Control Lists)
Nous verrons seulement la partie de configuration pour l'IPV4 et non pas l'IPV6.
Tout d'abord nous verrons ce que sont les ACLs, la logique de fonctionnement des ACL, les différents types d'ACL, nous verrons après cela comment configurer deux types d'ACL, le Standard numbered ACLs et le Standard named ACLs.

Les ACLs (Access Control Lists) ont différentes usages, dans les prochains cours nous verrons comment les utiliser pour un usage en sécurité.
Les ACLs fonctionnent comme des filtres de paquets qui informent le routeur lorsqu'il faut autoriser ou non le passage du trafique réseau.
Les ACLs peuvent filtrer le trafique basé sur la source/destination de l'adresse IP, source/destination d'un port de couche 4, etc.…

Nous utiliserons la topologie réseau suivante pour démontrer comment les ACLs fonctionnent :



A noter sur cette topologie :
- Les hôtes dans 192.168.1.0/24 peuvent accéder au réseau 10.0.1.0/24
- Les hôtes dans 192.168.2.0/24 ne peuvent pas accéder au réseau 10.0.1.0/24

- Les ACLs sont configurés en mode « global config mode » sur le routeur

Elles sont ordonnés en séquences de ACEs (Access Control Entries)
Par exemple pour l'ACL 1 :
1. Si l'IP Source est égal à 192.168.1.0/24 le trafique est autorisé
2. Si l'IP Source est égal à 192.168.2.0/24 le trafique est bloqué
3. Si l'IP Source est n'importe quoi d'autres le trafique est autorisé

Le routeur va exécuter les règles du trafique dans l'ordre, c'est pour cela qu'il est important de configurer le trafique dans l'ordre.
Configurer une ACL en mode « global config » ne rendra pas l'ACL effective automatiquement.
L'ACL doit être appliqué à une interface.
Les ACLs sont appliqués en Inbound ou Outbound (Connexion entrante ou sortante)

Imaginons que l'on veuille que :
- 192.168.1.0/24 ait accès à 10.0.1.0/24
- 192.168.2.0/24 ne puisse pas accéder à 10.0.1.0/24

Si l'on configure l'ACL sur l'interface G0/2 en Outbound (Sortant) du routeur R1, les conditions ne seront pas respectés, car le trafique sera filtré seulement pour les connexions sortantes donc lorsque 192.168.2.0/24 fera un ping vers 10.0.2.0/24 le trafique sera autorisé.
Si l'on configure l'ACL en Inbound (Entrant) le trafique sera filtré mais seulement pour le trafique en entrée donc lorsque 192.168.2.0/24 voudra faire un ping vers l'extérieur le trafique sera bloqué et 192.168.2.0/24 ne pourra communiquer qu'avec un autre PC du même réseau.

Le meilleur endroit ou placer l'ACL est l'interface G0/1 du routeur R2. Car a ce moment toutes les conditions sont respectés.

Donc une ACL est configuré en global config mode mais ils doivent être appliqués à une interface, lorsque cela est fais il faut spécifier une direction pour dire au routeur de vérifier les paquets qui entrent dans l'interface ou qui en sortent.
Les ACLs sont fais de 1 ou plusieurs ACEs.
Lorsque le routeur vérifie le paquet avec l'ACL, il les fais fonctionner les ACEs dans l'ordre, du plus haut vers le bas.
Si le paquet est compatible à unes des ACEs dans l'ACL, le routeur effectuera l'action et arrêtera de faire fonctionner l'ACL. Toutes les entrées à la suite de l'entrée compatible seront ignorés.

Par exemple s'il y a l'ACL suivante :
1. si IP source = 192.168.1.0/24 le trafique est autorisé
2. si IP source = 192.168.0.0/16 le trafique est bloqué

Si l'IP source est 192.168.1.1, le routeur prendra en compte seulement la première règle et autoriser le trafique et ne prendra pas en compte la deuxième.

Si à présent l'ACL est la suivante :
1. si IP source = 192.168.0.0/16 le trafique est bloqué
2. si IP source = 192.168.1.0/24 le trafique est autorisé

Si l'IP source est 192.168.1.1, le routeur va lire la première règle et bloquer le trafique sans prendre en compte la deuxième règle.

C'est pourquoi il est important de mettre les ACL dans l'ordre.
Une autre chose à préciser est que maximum une ACL peut être appliqué à une seule interface par direction.
Donc une ACL en Inbound (Entrante) et une ACL en Outbound (Sortante)

A présent voyons ce qu'il se passe si un paquet n'est en concordance avec aucune des ACL ?
Par exemple si une ACL est configuré avec les règles :
1. si l'IP source est 192.168.1.0/24 le trafique est autorisé
2. si l'IP source est 192.168.0.0/16 le trafique est bloqué

Si le routeur reçoit un paquet avec IP source de 10.0.0.1, cela n'est en concordance avec aucunes des règles de l'ACL. Par défaut le routeur bloquera le paquet, il ne le repartagera pas.
C'est ce que l'on appelle « implicit deny » ou « blocage implicite » en Français.

Maintenant que l'on a compris le fonctionnement des ACL, expliquons plus en détails les différents types d'ACL qui sont possibles.

Il y a deux types d'ACLs :

- Les ACL Standard : elles se basent sur l'adresse IP source uniquement, et sont composés de :
→ Standard Numbered ACLs
→ Standard Named ACLs

- Les ACL étendus : elles se basent sur l'adresse IP source/destination, port source/destination, etc.. et sont composés de :
→ Extended Numbered ACLs
→ Extended Named ACLs

Commençons par expliquer le fonctionnement des Standard Numbered ACLs :
Les Standard ACL se basent uniquement sur l'adresse IP source du paquet.
Les Numbered ACLs sont identifiés avec un chiffre (exemple : ACL1, ACL2, etc.…)

Différents types d'ACLs ont différents classements de nombre qui peuvent être utilisés :
→ Standard ACL peuvent utiliser 1-99 et 1300-1999
Voici un tableau qui présente le classement des ACL en nombre.

Protocol	Range
Standard IP	1–99 and 1300–1999
Extended IP	100–199 and 2000–2699
Ethernet type code	200–299
Ethernet address	700–799
Transparent bridging (protocol type)	200–299
Transparent bridging (vendor code)	700–799
Extended transparent bridging	1100–1199
DECnet and extended DECnet	300–399
Xerox Network Systems (XNS)	400–499
Extended XNS	500–599
AppleTalk	600–699
Source-route bridging (protocol type)	200–299
Source-route bridging (vendor code)	700–799
Internetwork Packet Exchange (IPX)	800–899
Extended IPX	900–999
IPX Service Advertising Protocol (SAP)	1000–1099

Voici la commande pour configurer une ACL standard numbered :
```
R1(config)#access-list number {deny | permit} ip wilcard-mask
```

Par exemple :
```
R1(config)#access-list 1 deny 1.1.1.1 0.0.0.0
```

Lorsque l'on veut ajouter une ACL avec un masque en /32 il n'est nécessaire de spécifier le masque 0.0.0.0 le routeur le configurera par défaut. Donc la commande précédente pourrait aussi être :
```
R1(config)#access-list 1 deny 1.1.1.1
```

Il existe une autre manière de configurer une ACL avec un masque en /32, en ajoute « host » entre l'adresse et l'autorisation (deny ou permit), la commande sera donc :
```
R1(config)#access-list 1 deny host 1.1.1.1
```

A présent que nous avons configuré l'ACL, il nous faut ajouter une règle pour autoriser tous les autres trafiques car sinon aucun trafique ne sera fonctionnel. On lance donc la commande :

```
R1(config)#access-list 1 permit any
```

Une autre possibilité pour autoriser tout le trafique restant serait d'utiliser la commande :
```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
```

Il est aussi possible d'ajouter une remarque sur une ACL par exemple avec la commande :
```
R1(config)#access-list 1 remark ##REMARQUE A AJOUTER##
```

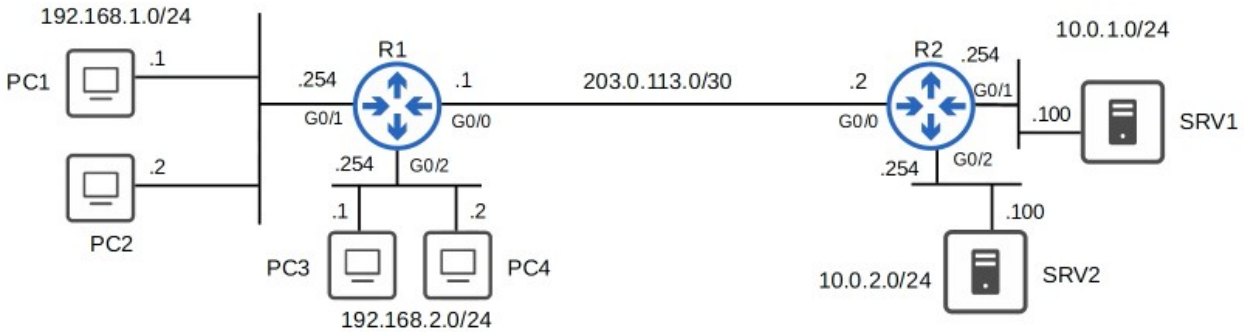
il est possible d'afficher les ACL du routeur en lançant unes de ces commandes :
```
R1(config)#do show access-lists
```

on peut aussi lancer cette commande :
```
R1(config)#do show ip access-lists
```

ou aussi celle ci :
```
R1(config)#do show running-config | include access-lists
```

Pour appliquer l'ACL à une interface on lance la commande :
```
R1(config-if)#ip access-group number {in | out}
```

Voyons à présent comment appliquer ces commandes sur un réseau définie :



avec les règles suivantes que l'on veut établir :
- PC1 peut accéder à 192.168.2.0/24
- Les autres PCs dans 192.168.1.0/24 ne peuvent pas accéder à 192.168.2.0/24

Il faudra appliquer les commandes suivantes sur le routeur R1 :
```
R1(config)#access-list 1 permit 192.168.1.1
R1(config)#access-list 1 deny 192 .168.1.0 0.0.0.255
R1(config)#access-list 1 permit any
R1(config)#interface g0/2
R1(config-if)#ip access-group 1 out
```

Les standard ACL doivent être appliqués le plus proche de la destination possible.
Le résultat de la commande pour voir l'ACL sera le suivant :

```
R1#show access-lists
Standard IP access list 1
    10 permit 192.168.1.1
    20 deny   192.168.1.0, wildcard bits 0.0.0.255
    30 permit any
R1#
```

Si le PC1 veut faire un ping de 192.168.2.1
Il prendra donc les ACL dans l'ordre en vérifiant d'abord la première règle qui est de permettre toute entrée venant de 192.168.1.1
comme ici l'IP source est 192.168.1.1 le routeur va autoriser le trafique.

A présent si le PC2 veut faire un ping vers PC3
Le routeur commencera par vérifier la première règle qui n'est pas en concordance
puis la deuxième règle qui dis que tout trafique provenant de 192.168.1.0/24 doit être bloqué.
Ici comme l'adresse IP source est 192.168.1.2 le trafique est bloqué.

Voyons à présent le fonctionnement des Standard Named ACLs.
Les Standard ACLs ne font fonctionner le trafique que en fonction de l'adresse IP source du paquet.
Les Named ACLs sont identifiés avec des noms (par exemple : « BLOCK JOE »)
Les Standard Named ACLs sont configurés en entrant en mode 'standard named ACL config mode', et en configurant chaque entrée dans ce mode config.
On utilise la commande suivante :

```
R1(config)#ip access-list standard acl-name
```

Une fois dans le mode Standard Named ACL on peut lancer la commande suivante :

```
R1(config-std-nacl)#[entry-number] {deny | permit} ip wilcard-mask
```

Un exemple de configuration de l'ACL sur le routeur R1 serait le suivant :

```
R1(config)#ip access-list standard BLOCK_BOB
R1(config-std-nacl)#5 deny 1.1.1.1
R1(config-std-nacl)#10 permit any
R1(config-std-nacl)#remark ##CONFIGURE LE 03  AOUT 2023##
R1(config-std-nacl)#interface g0/0
R1(config-if)#ip access-group BLOCK_BOB in
```

Essayons de configurer le Routeur pour que les conditions suivantes soit utilisés:
- Les PC dans 192.168.1.0/24 ne peuvent pas accéder à 10.0.2.0/24
- Le PC3 ne peut pas accéder à 10.0.1.0/24
- Les autres PC dans 192.168.2.0/24 peuvent accéder à 10.0.1.0/24
- Les autres PC dans 192.168.1.0/24 ne peuvent pas accéder à 10.0.1.0/24

les commandes à utiliser pourrait être les suivantes :

```
R2(config)#ip access-list standard TO_10.0.2.0/24
R2(config-std-nacl)#deny 192.168.1.0 0.0.0.255
R2(config-std-nacl)#permit any
R2(config-std-nacl)#interface g0/2
R2(config-if)#ip access-group TO_10.0.2.0/24 out
R2(config-std-nacl)#deny 192.168.2.1
R2(config-std-nacl)#permit 192.168.2.0 0.0.0.255
R2(config-std-nacl)#permit any
R2(config-std-nacl)#interface g0/1
R2(config-if)#ip access-group TO_10.0.1.0/24 out
```

Voici un résultat de la commande `show ip access-lists`

```
R2#show ip access-lists
Standard IP access list TO_10.0.1.0/24
    30 permit 192.168.1.1
    10 deny   192.168.2.1
    20 permit 192.168.2.0, wildcard bits 0.0.0.255
    40 deny   192.168.1.0, wildcard bits 0.0.0.255
    50 permit any
Standard IP access list TO_10.0.2.0/24
    10 deny   192.168.1.0, wildcard bits 0.0.0.255
    20 permit any
R2#
```

Une question que l'on pourrait se poser pourrait être pourquoi les ACL n'apparaissent pas dans l'ordre que celui ou l'on a lancer les commandes ?
La réponse est que le routeur réordonne les entrées en /32 d'abord, car cela permet d'améliorer le traitement de l'ACL, cela ne changera pas l'effet de l'ACL.
Cela s'applique pour les Standard Named et les Standard Numbered ACLs.
Par contre le logiciel Packet Tracer ne fera pas cela.