Packet Tracer - Configurer et modifier les listes ACLIPv4 standard.

Partie 1 : Vérifier la connectivité

Ping de PC A à PC D et PC C réussi

Ping de R1 à PC D et PC C réussi

Ping de PC C à PC A et PC B réussi

Ping de R3 a PC A et PC B réussi

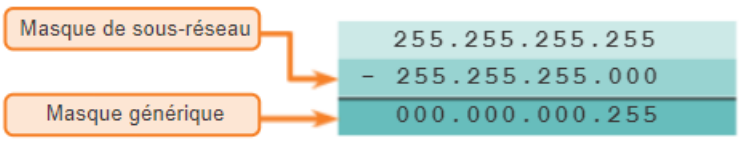
Tous les PC peuvent ping le serveur 209.165.200.254

Partie 2: Configurer et vérifier les ACL standard numérotées et nommées

Étape 1: Configurez une ACL standard numérotée.

Pour trouver le masque générique :

Calcul d'un masque générique pour /24



Donc le masque générique pour permettre à tous les hôtes sur le réseau 192.168.10.0/24 d'accéder au réseau 192.168.30.0/24 est 000.000.000.255

En suivant les bonnes pratiques, je placerai sur le routeur R3

Sur l'interface g0/0/0, et donc en sortie

a. Configurez l'ACL sur R3. Utilisez 1 pour le numéro de liste d'accès.

```
R3(config)# access-list 1 remark Allow R1 LANs Access
R3(config)# access-list 1 permit 192.168.10.0 0.0.0.255
R3(config)# access-list 1 permit 192.168.20.0 0.0.0.255
R3(config)# access-list 1 deny any
```

b. Appliquez la liste de contrôle d'accès à l'interface appropriée dans la bonne direction.

```
R3 (config) # interface g0/0/0
R3(config-if)# ip access-group 1 out
```

Pour afficher la liste 1 : show access-lists ou show access-lists 1 s'il y en a plusieurs

Pour afficher pour voir où la liste d'accès est appliquée et dans quelle direction : show ip interface g0/0/0

1) Sur R3, exécutez la commande **show access-lists 1** .

```
R3# show access-list 1
Standard IP access list 1
permit 192.168.10.0, wildcard bits 0.0.0.255
permit 192.168.20.0, wildcard bits 0.0.0.255
deny any
```

2) Sur R3, exécutez la commande **show ip interface g0/0/0** .

```
R3# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
Internet address is 192.168.30.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is 1
Inbound access list is not set
```

3) Le ping entre les réseaux 192.168.10.0/24 et le réseau 192.168.30.0/24, qui sont PC A et PC C, aboutit

4) Ping entre PC B et PC C aboutit

5) Les requêtes entre PC C et PC D ne devraient pas aboutir, PC D n'est pas autorisé, seulement le PC A et PC B. En effectuant le ping, on voit que ça ne marche pas.

6) Non, le ping depuis R1 vers PC C n'a pas fonctionné car R3 autorise seulement les réseaux 192.168.10.0/24 et 192.168.20.0/24

Étape 2 : Configurez une liste de contrôle d'accès standard nommée.

En suivant les bonnes pratiques, on la place sur le routeur R1

Sur l'interface g0/0/0

a. Créez la liste de contrôle d'accès nommée standard ACL BRANCH-OFFICE-POLICY sur R1.

```
R1(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# permit host 192.168.30.3
R1(config-std-nacl)# permit 192.168.40.0 0.0.0.255
R1(config-std-nacl)# end
R1#
*Feb 15 15:56:55.707: %SYS-5-CONFIG_I: Configured from console by console
```

Regardez le premier ACE dans la liste d'accès. Quelle est l'autre façon d'écrire cela ?

b. Appliquez la liste de contrôle d'accès à l'interface appropriée dans la bonne direction.

```
R1# config t
R1(config)# interface g0/0/0
R1(config-if)# ip access-group BRANCH-OFFICE-POLICY out
```

c. Vérifiez une liste de contrôle d'accès nommée.

1) Sur R1, exécutez la commande show access-lists .

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
10 permit host 192.168.30.3
20 permit 192.168.40.0 0.0.0.255
```

Y a-t-il une différence entre cette liste de contrôle d'accès sur R1 et la liste de contrôle d'accès sur R3? Le cas échéant, quelle est-elle?

2) Sur R1, exécutez la commande **show ip interface g0/0/0** pour vérifier la liste de contrôle d'accès sur l'interface.

```
R1# show ip interface g0/0/0
GigabitEthernet0/0/0 is up, line protocol is up (connected)
Internet address is 192.168.10.1/24
Broadcast address is 255.255.255.255
Address determined by setup command
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing access list is BRANCH-OFFICE-POLICY
Inbound access list is not set
```

a) permis 192.168.30.3 0.0.0.0

c) Oui, il y a une différence : les IPs host, le nom et pas de 30 deny any

Test de la liste d'accès PC C ping bien PC A

3) Testez la liste de contrôle d'accès pour vous assurer que seul l'hôte PC-C soit autorisé à accéder au réseau 192.168.10.0/24. Vous devez effectuer une requête ping étendue et utiliser l'adresse G0/0/0 sur R3 comme source. Envoyez une requête ping à l'adresse IP de PC-A.

```
R3# ping
Protocol [ip]:
Target IP address: 192.168.10.3
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.30.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:
Packet sent with a source address of 192.168.30.1
U.U.U
```

Les requêtes ping ont-elles abouti ?

Les requêtes ping n'ont pas abouti

4) Le ping de PC D vers PC A abouti la liste de contrôle autorise le trafic entre le réseau 192.168.40.0/24 et le réseau 192.168.10.0/24.

Partie 3: Modifier une liste de contrôle d'accès standard

OPTION 1: Exécutez une commande **no ip access-list standard BRANCH-OFFICE-POLICY** en mode de configuration globale. Cela supprimerait l'ACL du routeur. Selon l'IOS du routeur, l'un des scénarios suivants se produirait: tout filtrage des paquets serait annulé et tous les paquets seraient autorisés à transiter par le routeur; ou, parce que vous n'avez pas supprimé la commande **ip access-group** sur l'interface G0/1, le filtrage serait toujours en place. Quoi qu'il en soit, lorsque la liste de contrôle d'accès a disparu, vous pouvez la retaper dans son intégralité, ou la copier et la coller à partir d'un éditeur de texte.

OPTION 2: Vous pouvez modifier les listes de contrôle d'accès existantes en ajoutant ou en supprimant des lignes spécifiques dans la liste elle-même. Cela peut être pratique, en particulier avec des listes de contrôle d'accès comportant de nombreuses lignes de code. Le fait de retaper la liste de contrôle d'accès entière ou de la copier et coller peut facilement engendrer des erreurs. La modification de lignes spécifiques dans la liste de contrôle d'accès est facile à effectuer.

Là on utilise l'option 2

Étape 1: Modifiez une liste de contrôle d'accès standard nommée. .

a. À partir de R1, exécutez la commande **show access-lists** .

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
10 permit 192.168.30.3 (8 matches)
20 permit 192.168.40.0 0.0.0.255 (5 matches)
```

b. Ajoutez deux lignes supplémentaires à la fin de la liste de contrôle d'accès. À partir du mode de configuration globale, modifiez la liste de contrôle d'accès, BRANCH-OFFICE-POLICY.

```
R1#(config)# ip access-list standard BRANCH-OFFICE-POLICY
R1(config-std-nacl)# 30 permit 209.165.200.224 0.0.0.31
R1(config-std-nacl)# 40 deny any
R1(config-std-nacl)# end
```

c. Vérifiez la liste de contrôle d'accès.

1) Sur R1, exécutez la commande **show access-lists** .

```
R1# show access-lists
Standard IP access list BRANCH-OFFICE-POLICY
10 permit 192.168.30.3 (8 matches)
20 permit 192.168.40.0, wildcard bits 0.0.0.255 (5 matches)
30 permit 209.165.200.224, wildcard bits 0.0.0.31
40 deny any
```

Devez-vous appliquer la liste BRANCH-OFFICE-POLICY à l'interface G0/1 sur R1?

2) Testez la liste de contrôle d'accès pour voir si elle permet le trafic du réseau 209.165.200.224/27 pour retourner au réseau 192.168.10.0/24. À partir de PC-A, envoyez une requête ping vers le serveur à 209.165.200.254.

Les requêtes ping ont-elles abouti ?

c)Non, la commande **ip access-group BRANCH-OFFICE-POLICY out** est toujours en place sur G0/1.

Les pings de PCA vers le serveur ont abouti

Question de réflexion :

1) Les ACL standard ne peuvent filtrer qu'en fonction de l'adresse source. Ils autorisent ou refusent tout (tous les protocoles et services). Les listes de contrôle d'accès étendues, bien que plus difficiles à écrire, sont bien adaptées aux réseaux complexes où vous devrez peut-être autoriser le trafic pour que certains ports de couche 4 aient accès aux réseaux tout en en refusant d'autres. De plus, les ACL standard doivent être appliquées aussi près que possible de la destination. Cela permet au trafic inutile d'utiliser la bande passante du réseau. Les listes de contrôle d'accès étendues peuvent bloquer le trafic à proximité de la source. Cela empêche le trafic inutile de se rendre à la destination où il est bloqué.