Packet Tracer - Configurer et modifier les listes ACL IPv4 standard

# Table d'adressage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appareil | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| R1 | G0/0/0 | 192.168.10.1 | 255.255.255.0 | N/A |
| R1 | G0/0/1 | 192.168.20.1 | 255.255.255.0 | N/A |
| R1 | S0/1/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/A |
| Périphérie | S0/1/0 | 10.1.1.2 | 255.255.255.252 | N/A |
| Périphérie | S0/1/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/A |
| Périphérie | S0/2/1 | 209.165.200.225 | 255.255.255.224 | N/A |
| R3 | G0/0/0 | 192.168.30.1 | 255.255.255.0 | N/A |
| R3 | G0/0/1 | 192.168.40.1 | 255.255.255.0 | N/A |
| R3 | S0/1/1 | 10.2.2.1 | 255.255.255.252 | N/A |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S2 | VLAN 1 | 192.168.20.11 | 255.255.255.0 | 192.168.20.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| S4 | VLAN 1 | 192.168.40.11 | 255.255.255.0 | 192.168.40.1 |
| PC-A | Carte réseau | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-B | Carte réseau | 192.168.20.3 | 255.255.255.0 | 192.168.20.1 |
| PC-C | Carte réseau | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |
| PC-D | Carte réseau | 192.168.40.3 | 255.255.255.0 | 192.168.40.1 |

# Objectifs

Partie 1: Vérifier la connectivité

Partie 2: Configurer et vérifier les listes de contrôle d'accès numérotées et nommées standard

Partie 3: Modifier une Liste ACL standard

# Contexte/scénario

La sécurité du réseau et le contrôle des flux de trafic sont des problèmes importants lors la conception et 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 deux sites d'entreprises représentés par R1 et R3. La direction a établi certaines stratégies d'accès entre les LAN situés au niveau de R1 et R3, que vous devez implémenter. Le routeur périphérique ISP situé entre R1 et R3 ne comportera aucune liste de contrôle d'accès. Aucun accès administratif ne serait autorisé à un routeur périphérique étant donné que vous pouvez uniquement contrôler et gérer votre propre matériel.

# Instructions

## Vérifier la connectivité

Dans la partie 1, vous 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. Assurez-vous que votre réseau fonctionne correctement avant de commencer à filtrer le trafic.

#### Questions:

À partir de PC-A, envoyez une requête ping PC-C et PC-D.Vos pings ont-ils abouti?

À partir de R1, envoyez une requête ping PC-C et PC-D. Vos pings ont-ils abouti?

À partir de PC-C, envoyez une requête ping à PC-A et PC-B.Vos pings ont-ils abouti ?

À partir de R3, envoyez une requête ping PC-A et PC-B. Vos pings ont-ils abouti ?

Tous les PC peuvent-ils envoyer une requête ping au serveur 209.165.200.254 ?

## Configurer et vérifier les listes de contrôle d'accès numérotées et nommées standard

### Configurez une liste de contrôle d'accès standard numérotée.

Les listes de contrôle d'accès standard filtrent le trafic en fonction de l'adresse IP de la source. L'une des meilleures pratiques typique pour les listes de contrôle d'accès standard consiste à la configurer et l'appliquer aussi près que possible de la destination. Pour la première liste de contrôle d'accès dans cettte exercise, créez une liste de contrôle d'accès numérotée standard qui autorise le trafic de tous les hôtes du réseau 192.168.10.0/24 et de tous les hôtes du réseau 192.168.20.0/24 pour accéder à tous les hôtes du réseau 192.168.30.0/24. La stratégie de sécurité indique également qu'une entrée de contrôle d'accès (ACE) **deny any** , également appelée instruction ACL, doit figurer à la fin de toutes listes de contrôle d'accès.

#### Questions:

Quel masque générique utiliseriez-vous pour permettre à tous les hôtes sur le réseau 192.168.10.0/24 d'accéder au réseau 192.168.30.0/24?

En suivant les meilleures pratiques recommandées par Cisco, sur quel routeur placeriez-vous cette liste de contrôle d'accès?

Sur quelle interface placeriez-vous cette liste de contrôle d'accès? Dans quelle direction l'appliqueriez-vous?

* + - 1. Configurez la liste de contrôle d'accès sur R3. Utilisez 1 pour le numéro de liste d'accès.

Ouvrez la fenêtre de configuration.

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**

* + - 1. 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**

* + - 1. Vérifiez une liste de contrôle d'accès numérotée.

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.

#### Questions:

Pour afficher la liste d'accès 1 dans son intégralité avec toutes les listes d'ACE, quelle commande utiliseriez-vous?

Quelle commande utiliseriez-vous pour savoir où la liste d'accès a été appliquée et dans quelle direction?

* + - * 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

* + - * 1. 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

<Output omitted>

#### Questions:

* + - * 1. Testez la liste de contrôle d'accès pour voir si elle autorise le trafic entre le réseau 192.168.10.0/24 et le réseau 192.168.30.0/24.

À partir de l'invite de commande de PC-A, envoyez une requête ping à l'adresse IP de PC-C. Les requêtes ping ont-elles abouti?

* + - * 1. Testez la liste de contrôle d'accès pour voir si elle autorise le trafic entre le réseau 192.168.20.0/24 et le réseau 192.168.30.0/24.

À partir de l'invite de commande de PC-B, envoyez une requête ping à l'adresse IP de PC-C. Les requêtes ping ont-elles abouti?

* + - * 1. Les requêtes pings de PC-D vers PC-C devraient-ils aboutir ? Envoyez une requête ping de PC-D vers PC-C pour vérifier votre réponse.
      1. À partir de l'invite de R1, envoyez une requête ping à l'adresse IP de PC-C.

R1# **ping 192.168.30.3**

#### Question:

La requête ping a-t-elle abouti? Expliquez votre réponse.

* + - 1. Exécutez à nouveau la commande **show access-lists 1** . Notez que la sortie de la commande affiche des informations sur le nombre de fois que chaque ACE a été mis en correspondance par le trafic qui a atteint l'interface Gigabit Ethernet 0/0/0.

R3# **show access-lists 1**

Standard IP access list 1

permit 192.168.10.0 0.0.0.255 (4 match(es))

permit 192.168.20.0 0.0.0.255 (4 match(es))

deny any (4 match(es))

### Configurez une liste de contrôle d'accès standard nommée.

Créez une liste de contrôle d'accès standard nommée conformément à la stratégie suivante: autoriser le trafic de tous les hôtes sur 192.168.40.0/24 à accéder à tous les hôtes sur le réseau 192.168.10.0/24. En outre, autorisez uniquement les accès du PC-C hôte au réseau 192.168.10.0/24. Cette liste d'accès devrait s'appeler BRANCH-OFFICE-POLICY.

#### Questions:

En suivant les meilleures pratiques recommandées par Cisco, sur quel routeur placeriez-vous cette liste de contrôle d'accès?

Sur quelle interface placeriez-vous cette liste de contrôle d'accès? Dans quelle direction l'appliqueriez-vous?

* + - 1. 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

#### Question:

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

* + - 1. Appliquez la liste de contrôle d'accès à l'interface appropriée dans la bonne direction.

R1# **config t**

R1 (config) # **interface g0/0/1**

R1(config-if)# **ip access-group BRANCH-OFFICE-POLICY out**

* + - 1. 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

#### Question:

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?

* + - * 1. Sur R1, exécutez la commande **show ip interface g0/0/0** pour vérifier que lliste de contrôle d'accès est configurée sur l'interface.

R1# **montrer l'interface ip 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

La liste d’accès sortante est BRANCH-OFFICE-POLICY

Inbound access list is not set

<Output omitted>

#### Question:

Testez la liste de contrôle d'accès. À partir de l'invite de commande de PC-C, envoyez une requête ping à l'adresse IP de PC-A. A-t-elle abouti?

* + - * 1. Testez la liste de contrôle d'accès pour vous assurer que seul l'hôte PC-C soit autorisé à accéder au 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

#### Question:

Les requêtes ping ont-elles abouti?

* + - * 1. Testez la liste de contrôle d'accès pour voir si elle autorise le trafic entre le réseau 192.168.40.0/24 et le réseau 192.168.10.0/24. À partir de l'invite de commande de PC-D,envoyez une requête ping à l'adresse IP de PC-A.

#### Question:

Les requêtes ping ont-elles abouti?

Fermez la fenêtre de configuration.

## Modifier une liste de contrôle d'accès standard

En entreprise, il est courant que les stratégies de sécurité évoluent. Pour cette raison, les listes de contrôle d'accès peuvent être modifiées. Dans la partie 3, vous allez modifier l’une des listes de contrôle d’accès que vous avez précédemment configurées pour l’adapter à la nouvelle politique de direction mise en place.

Essayez d'envoyer un ping au serveur 209.165.200.254 à partir de PC-A. Notez que le ping n'a pas réussi. L'ACL sur R1 empêche le trafic Internet de revenir sur PC-A. Cela est dû au fait que l'adresse source dans les paquets renvoyés n'est pas dans la plage des adresses autorisées.

La direction a décidé que les utilisateurs du réseau 209.165.200.224/27 devait disposer d'un accès intégral au réseau192.168.10.0/24. La direction veut également que les listes de contrôle d'accès sur tous ses routeurs suivent des règles cohérentes. Une entrée de contrôle d'accès **deny any** doit être placée à la fin de toutes les listes de contrôle d'accès. Vous devez modifier la liste de contrôle d'accès BRANCH-OFFICE-POLICY.

Vous allez ajouter deux lignes supplémentaires à cette liste de contrôle d'accès. Il existe deux manières de le faire:

**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-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-coller peut facilement engendrer des erreurs. La modfication de lignes spécifiques dans la liste de contrôle d'accès est facile à effectuer.

Pour cette activité, utilisez l'option 2.

### Modifiez une liste de contrôle d'accès standard nommée.

* + - 1. À partir de R1, exécutez la commande **show access-lists** .

Ouvrez la fenêtre de configuration.

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)

* + - 1. 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**

* + - 1. 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

#### Question:

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

Saisissez vos réponses ici

* + - * 1. 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.

#### Question:

Les requêtes ping ont-elles abouti?

Fermez la fenêtre de configuration.

## Questions de réflexion

* 1. Comme vous pouvez le constater, les listes de contrôle d'accès standard sont particulièrement puissantes et fonctionnent très bien. Pourquoi auriez-vous jamais besoin d'utiliser les listes de contrôle d'accès étendues?
  2. Il y a plus d'éléments à taper lors de l'utilisation d'une liste de contrôle d'accès nommée par opposition à une liste de contrôle d'accès numérotée. Pour quelle raison choisiriez-vous des listes de contrôle d'accès nommées plutôt que des listes d'accès numérotées?

Saisissez v