Packet Tracer - Configurer les listes de contrôle d'accès étendues - Scénario 2

# Table d'adressage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appareil | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| RT1 | G0/0 | 172.31.1.126 | 255.255.255.224 | N/A |
| RT1 | S0/0/0 | 209.165.1.2 | 255.255.255.252 | N/A |
| PC1 | Carte réseau | 172.31.1.101 | 255.255.255.224 | 172.31.1.126 |
| PC2 | Carte réseau | 172.31.1.102 | 255.255.255.224 | 172.31.1.126 |
| PC3 | Carte réseau | 172.31.1.103 | 255.255.255.224 | 172.31.1.126 |
| Serveur 1 | Carte réseau | 64.101.255.254 |  |  |
| Serveur 2 | Carte réseau | 64.103.255.254 |  |  |

# Objectifs

Partie 1: Configurer une liste de contrôle d'accès ACL étendue nommée

Partie 2: Appliquer et vérifier la liste de contrôle d'accès ACL étendue

# Contexte/scénario

Dans ce scénario, certains appareils du LAN sont autorisés à accéder à différents services sur des serveurs sur Internet.

# Instructions

## Configurer une liste de contrôle d'accès ACL étendue nommée

Configurez une liste de contrôle d'accès nommée pour implémenter la stratégie suivante:

* Bloquer les accès HTTP et HTTPS de **PC1** au **Serveur 1** et **Serveur 2.** Les serveurs sont dans le cloud et vous êtes la seule personne qui connaît leur adresse IP.
* Bloquer l'accès FTP de **PC2** au **Serveur 1** et **Serveur 2**.
* Bloquez l'accès ICMP de **PC3** au **Serveur 1** et **Serveur 2**.

**Remarque:** À des fins d'évaluation, vous devez configurer les instructions dans l'ordre indiqué dans les étapes suivantes.

### Refusez à PC1 l'accès aux services HTTP et HTTPS sur Serveur1 et Serveu` r2.

* + - 1. Créez une liste de contrôle d'accès IP nommée qui empêchera **PC1** d'accéder aux services HTTP et HTTPS de **Serveur 1** et **Serveur 2**. Quatre instructions de contrôle d'accès sont requises.

#### Question:

Quelle est la commande pour commencer la configuration d'une liste d'accès étendue avec le nom **ACL**?

Ouvrez la fenêtre de configuration.

* + - 1. Commencez la configuration d'ACL avec une déclaration qui refuse l’accès de **PC1** au **Serveur 1**, uniquement pour HTTP (port 80). Consultez le tableau d'adressage pour l'adresse IP de **PC1** et **Serveur 1**.

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 80**

* + - 1. Ensuite, saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur 1**, uniquement pour HTTPS (port 443).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.101.255.254 eq 443**

* + - 1. Saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur 2**, uniquement pour HTTP. Consultez la table d'adressage pour l'adresse IP de **Serveur 2.**

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 80**

* + - 1. Saisissez la déclaration qui refuse l'accès du **PC1** au **Serveur 2**, uniquement pour HTTP.

RT1(config-ext-nacl)# **deny tcp host 172.31.1.101 host 64.103.255.254 eq 443**

### Refusez à PC2 l'accès aux services FTP sur Serveur 1 et Serveur 2.

Consultez la table d'adressage pour l'adresse IP de **PC2**.

* + - 1. Saisissez la déclaration qui refuse l'accès du **PC2** au **Serveur 1**, uniquement pour FTP (port 21 seulement).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.101.255.254 eq 21**

* + - 1. Saisissez la déclaration qui refuse l'accès du **PC2** au **Serveur 2**, uniquement pour FTP (port 21 seulement).

RT1(config-ext-nacl)# **deny tcp host 172.31.1.102 host 64.103.255.254 eq 21**

### Empêchez PC3 d'envoyer une requête ping à Serveur 1 et Serveur 2.

Consultez la table d'adressage pour l'adresse IP de **PC3.**

* + - 1. Saisissiez la déclaration qui refuse l'accès ICMP de **PC3** vers **Serveur 1**.

RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.101.255.254**

* + - 1. Saisissiez la déclaration qui refuse l'accès ICMP de **PC3** vers **Serveur 2**.

RT1(config-ext-nacl)# **deny icmp host 172.31.1.103 host 64.103.255.254**

### Autorisez tout autre trafic IP.

Par défaut, une liste d'accès refuse tout trafic qui ne correspond à aucune règle de la liste. Saisissiez la commande qui autorise tout le trafic qui ne correspond à aucune des instructions de liste d'accès configurées.

### Vérifiez la configuration de la liste d'accès avant de l'appliquer à une interface.

Avant d'appliquer une liste d'accès, la configuration doit être vérifiée pour s'assurer qu'il n'y a pas d'erreurs typographiques et que les déclarations sont dans le bon ordre. Pour afficher la configuration actuelle de la liste d'accès, utilisez la commande **show access-lists** ou **show running-config** .

RT1# **show access-lists**

Extended IP access list ACL

10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www

20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443

30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www

40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443

50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp

60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp

70 deny icmp host 172.31.1.103 host 64.101.255.254

80 deny icmp host 172.31.1.103 host 64.103.255.254

90 permit ip any any

RT1# **show running-config | begin access-list**

ip access-list extended ACL

deny tcp host 172.31.1.101 host 64.101.255.254 eq www

deny tcp host 172.31.1.101 host 64.101.255.254 eq 443

deny tcp host 172.31.1.101 host 64.103.255.254 eq www

deny tcp host 172.31.1.101 host 64.103.255.254 eq 443

deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp

deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp

deny icmp host 172.31.1.103 host 64.101.255.254

deny icmp host 172.31.1.103 host 64.103.255.254

permit ip any any

Fermez la fenêtre de configuration.

**Remarque**: La différence entre la sortie de la commande **show access-lists** et la sortie de la commande **show running-config** est que la commande **show access-lists** inclut les numéros de séquence attribués à la commande instructions de configuration. Ces numéros de séquence permettent la modification, la suppression et l'insertion de lignes uniques dans la configuration de la liste d'accès. Les numéros de séquence définissent également l'ordre de traitement des instructions de contrôle d'accès individuelles, en commençant par le numéro de séquence le plus bas.

## Appliquer et vérifier la liste de contrôle d'accès étendue

Le trafic à filtrer provient du réseau 172.31.1.96/27 et est à destination des réseaux distants. L'emplacement approprié de la liste de contrôle d'accès dépend également de la relation du trafic par rapport à **RT1**. En général, les listes d'accès étendues doivent être placées sur l'interface la plus proche de la source du trafic.

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

**Remarque**: Dans un réseau opérationnel réel, une ACL non testée ne doit jamais être appliquée à une interface active. Ce n'est pas une bonne pratique et peut perturber le fonctionnement du réseau.

#### Question:

Sur quelle interface l'ACL nommée doit-elle être appliquée et dans quelle direction?

Ouvrez la fenêtre de configuration.

Passez en mode de configuration de commandes pour appliquer la liste de contrôle d'accès à l'interface.

### Testez l'accès pour chaque PC.

* + - 1. Accédez aux sites web de **Serveur 1** et **Serveur 2** en utilisant le navigateur web de **PC1.** Utilisez les protocoles HTTP et HTTPS. Utilisez la commande **show access-lists** pour afficher l'instruction liste d'accès autorisée ou refusée au trafic. La sortie de la commande **show access-lists** affiche le nombre de paquets correspondant à chaque instruction depuis la dernière fois que les compteurs ont été effacés ou que le routeur a redémarré.

**Remarque**: Pour effacer les compteurs d'une liste d'accès, utilisez la commande **clear access-list counters** .

RT1#**show ip access-lists**

Extended IP access list ACL

10 deny tcp host 172.31.1.101 host 64.101.255.254 eq www (12 match(es))

20 deny tcp host 172.31.1.101 host 64.101.255.254 eq 443 (12 match(es))

30 deny tcp host 172.31.1.101 host 64.103.255.254 eq www

40 deny tcp host 172.31.1.101 host 64.103.255.254 eq 443

50 deny tcp host 172.31.1.102 host 64.101.255.254 eq ftp

60 deny tcp host 172.31.1.102 host 64.103.255.254 eq ftp

70 deny icmp host 172.31.1.103 host 64.101.255.254

80 deny icmp host 172.31.1.103 host 64.103.255.254

90 permit ip any any

Fermez la fenêtre de configuration.

* + - 1. Accédez aux services FTP de **Serveur 1** et **Serveur 2** en utilisant **PC1**. Le nom d'utilisateur et le mot de passe sont **cisco**.
      2. Envoyez une requête ping à **Serveur 1** et **Serveur 2** depuis **PC1**.
      3. Répétez les étapes 2a à 2c avec **PC2** et **PC3** pour vérifier le bon fonctionnement de la liste d'accès.

Fin du documen