Packet Tracer - Configurer les ACL étendues - Scénario 1

# Table d'adressage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Appareil | Interface | Adresse IP | Masque de sous-réseau | Passerelle par défaut |
| R1 | G0/0 | 172.22.34.65 | 255.255.255.224 | N/A |
| R1 | G0/1 | 172.22.34.97 | 255.255.255.240 | N/A |
| R1 | G0/2 | 172.22.34.1 | 255.255.255.192 | N/A |
| Serveur | Carte réseau | 172.22.34.62 | 255.255.255.192 | 172.22.34.1 |
| PC1 | Carte réseau | 172.22.34.66 | 255.255.255.224 | 172.22.34.65 |
| PC2 | Carte réseau | 172.22.34.98 | 255.255.255.240 | 172.22.34.97 |

# Objectifs

Partie 1: Configurer, appliquer et vérifier une liste de contrôle d'accès numérotée étendue

Partie 2: Configurer, appliquer et vérifier une liste de contrôle d'accès nommée étendue

# Contexte/scénario

Deux employés ont besoin d'accéder aux services fournis par le serveur. **PC1** a uniquement besoin d'un accès FTP tandis que **PC2** a uniquement besoin d'un accès web. Les deux ordinateurs peuvent envoyer une requête ping au serveur, mais pas entre eux.

# Instructions

## Configurer, appliquer et vérifier une liste de contrôle d'accès numérotée étendue

### Configurez un ACL pour autoriser le FTP et l'ICMP à partir du LAN du PC1.

* + - 1. En mode de configuration globale sur **R1**, entrez la commande suivante pour déterminer le premier numéro valide d'une liste de contrôle d'accès étendue.

Ouvrez la fenêtre de configuration.

R1(config)# **access-list ?**

<1-99> IP standard access list

<100-199> IP extended access list

* + - 1. Ajoutez **100** à la commande et faites suivre d'un point d'interrogation.

R1(config)# **access-list 100 ?**

deny Specify packets to reject

permit Specify packets to forward

remark Access list entry comment

* + - 1. Pour autoriser le trafic FTP, tapez **permit,** suivi d'un point d'interrogation.

R1(config)# **access-list 100 permit ?**

ahp Authentication Header Protocol

eigrp Cisco's EIGRP routing protocol

esp Encapsulation Security Payload

gre Cisco's GRE tunneling

icmp Internet Control Message Protocol

ip Any Internet Protocol

ospf OSPF routing protocol

tcp Transmission Control Protocol

udp User Datagram Protocol

* + - 1. Lorsqu'elle est configurée et appliquée, cette ACL devrait permettre le FTP et l'ICMP. ICMP est indiqué ci-dessus, mais FTP non. En effet, FTP est un protocole de couche d'application qui utilise TCP au niveau de la couche de transport. Entrez TCP pour affiner l'aide ACL.

R1(config)# **access-list 100 permit tcp ?**

A.B.C.D Source address

any Any source host

host A single source host

* + - 1. L'adresse source peut représenter un seul périphérique, tel que PC1, à l'aide du mot-clé **host** , puis de l'adresse IP de PC1. L'utilisation du mot-clé **any** permet n'importe quel hôte sur n'importe quel réseau. Le filtrage peut également être effectué par une adresse réseau. Dans ce cas, il s'agit de tout hôte qui possède une adresse appartenant au réseau 172.22.34.64/27. Saisissez cette adresse de réseau, suivie d'un point d'interrogation.

R1(config)# **access-list 100 permit tcp 172.22.34.64 ?**

A.B.C.D Source wildcard bits

* + - 1. Calculate the wildcard mask by determining the binary opposite of the /27 subnet mask.

**11111111.11111111.11111111.111**00000 = 255.255.255.224

00000000.00000000.00000000.000**11111** = 0.0.0.31

* + - 1. Tapez le masque générique suivi d'un point d'interrogation.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 ?**

A.B.C.D Destination address

any Any destination host

eq Match only packets on a given port number

gt Match only packets with a greater port number

host A single destination host

lt Match only packets with a lower port number

neq Match only packets not on a given port number

range Match only packets in the range of port numbers

* + - 1. Configurez l'adresse de destination. Dans ce scénario, nous filtrons le trafic pour une seule destination, qui est le serveur. Saisissez le mot clé host suivi de l'adresse IP du serveur.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 ?**

dscp Match packets with given dscp value

eq Match only packets on a given port number

established established

gt Match only packets with a greater port number

lt Match only packets with a lower port number

neq Match only packets not on a given port number

precedence Match packets with given precedence value

range Match only packets in the range of port numbers

<cr>

* + - 1. Notez que l'une des options est **<cr>** (retour chariot). Autrement dit, vous pouvez appuyer sur **Entrée** et l'instruction autoriserait tout le trafic TCP. Néanmoins, nous n'autorisons que le trafic FTP; en conséquence, saisissez le mot clé **eq** suivi d'un point d'interrogation pour afficher les options possibles. Ensuite, saisissez **ftp** et appuyez sur **Enter**.

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ?**

<0-65535> Port number

ftp File Transfer Protocol (21)

pop3 Post Office Protocol v3 (110)

smtp Simple Mail Transport Protocol (25)

telnet Telnet (23)

www World Wide Web (HTTP, 80)

R1(config)# **access-list 100 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp**

* + - 1. Créez une deuxième instruction de liste d'accès pour autoriser le trafic ICMP (ping, etc.) entre PC1 et le serveur. Notez que le numéro de la liste d'accès reste le même et qu'il n'est pas nécessaire d'indiquer un type de trafic ICMP spécifique.

R1(config)# **access-list 100 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62**

* + - 1. Par défaut, tout autre trafic est refusé.
      2. Exécutez la commande **show access-list** et vérifiez que la liste d'accès 100 contient les instructions correctes. Notez que la déclaration **deny any any** n'apparaît pas à la fin de la liste d'accès. L'exécution par défaut d'une liste d'accès est que si un paquet ne correspond pas à une instruction dans la liste d'accès, il n'est pas autorisé via l'interface.

R1# **show** access-lists

Extended IP access list 100

10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

### Appliquez la liste de contrôle d'accès sur l'interface appropriée pour filtrer le trafic.

Du point de vue de **R1**, le trafic auquel s'applique la liste de contrôle d'accès 100 est entrant depuis le réseau connecté à l'interface Gigabit Ethernet 0/0. Passez en mode de configuration d'interface et appliquez la liste de contrôle d'accès.

**Remarque**: Sur un réseau opérationnel réel, il n'est pas recommandé d'appliquer une liste d'accès non testée à une interface active.

R1(config)# **interface gigabitEthernet 0/0**

R1(config-if)# **ip access-group 100 in**

### Vérifiez l'implémentation de la liste de contrôle d'accès.

* + - 1. Envoyez une requête ping de PC1 au serveur. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.
      2. Établissez une connexion FTP entre PC1 et le serveur. Le nom d'utilisateur et le mot de passe sont **cisco** dans les deux cas.

PC> **ftp 172.22.34.62**

* + - 1. Quittez le service FTP.

ftp> **quit**

Fermez la fenêtre de configuration.

* + - 1. Envoyez une requête ping de PC1 vers PC2. L'hôte de destination doit être injoignable,car la ACL n'a pas explicitement autorisé le trafic.

## Configurer, appliquer et vérifier une liste de contrôle d'accès nommée étendue

### Configurez une liste de contrôle d'accès pour autoriser l'accès HTTP et ICMP à partir du LAN du PC2.

* + - 1. Les listes de contrôle d'accès nommées commencent par le mot-clé **ip**. En mode de configuration globale sur **R1**, entrez la commande suivante suivie d'un point d'interrogation.

Ouvrez la fenêtre de configuration.

R1(config)# **ip access-list ?**

extended Extended Access List

standard Standard Access List

* + - 1. Vous pouvez configurer des listes de contrôle d'accès étendues et nommées standard. Cette liste d'accès filtre les adresses IP source et de destination; par conséquent, elle doit être étendue. Saisissez **HTTP\_ONLY** comme nom. (Pour la notation Packet Tracer, le nom est sensible à la casse et les instructions de liste d'accès doivent être dans l'ordre correct.)

R1(config)# **ip access-list extended HTTP\_ONLY**

* + - 1. L'invite change. Vous êtes maintenant en mode de configuration de liste de contrôle d'accès nommée étendue. Tous les appareils sur le réseau LAN de **PC2** ont besoin d'un accès TCP. Saisissez l'adresse du réseau, suivie d'un point d'interrogation.

R1(config-ext-nacl)# **permit tcp 172.22.34.96 ?**

A.B.C.D Source wildcard bits

* + - 1. Une autre manière de calculer un masque générique est de soustraire le masque de sous-réseau de 255.255.255.255.

255.255.255.255

- 255.255.255.240

-----------------

= 0. 0. 0. 15

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15**

* + - 1. Terminez l'instruction en spécifiant l'adresse du serveur comme vous l'avez fait dans la Partie 1 et en filtrant le trafic **www**.

R1(config-ext-nacl)# **permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www**

* + - 1. Créez une deuxième instruction de liste d'accès pour autoriser le trafic ICMP (ping, etc.) entre **PC2** et **Serveur**. Remarque: L'invite reste identique et un type de trafic ICMP spécifique n'a pas besoin d'être spécifié.

R1(config-ext-nacl)# **permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62**

* + - 1. Par défaut, tout autre trafic est refusé. Quittez le mode de configuration de liste de contrôle d'accès étendue nommée.
      2. Exécutez la commande **show access-list** et vérifiez que la liste d'accès **HTTP\_ONLY** contient les instructions correctes.

R1# **show access-lists**

Extended IP access list 100

10 permit tcp 172.22.34.64 0.0.0.31 host 172.22.34.62 eq ftp

20 permit icmp 172.22.34.64 0.0.0.31 host 172.22.34.62

Extended IP access list HTTP\_ONLY

10 permit tcp 172.22.34.96 0.0.0.15 host 172.22.34.62 eq www

20 permit icmp 172.22.34.96 0.0.0.15 host 172.22.34.62

### Appliquez la liste de contrôle d'accès sur l'interface appropriée pour filtrer le trafic.

Du point de vue de **R1**, le trafic auquel s'applique la liste de contrôle d'accès **HTTP\_ONLY** est entrant depuis le réseau connecté à l'interface Gigabit Ethernet 0/1. Passez en mode de configuration d'interface et appliquez la liste de contrôle d'accès.

**Remarque**: Sur un réseau opérationnel réel, il n'est pas recommandé d'appliquer une liste d'accès non testée à une interface active. Il devrait être évité si possible.

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

R1(config-if)# **ip access-group HTTP\_ONLY in**

### Vérifiez l'implémentation de la liste de contrôle d'accès.

* + - 1. Envoyez une requête ping de **PC2** au **Server**. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.
      2. Depuis le PC2, ouvrez un navigateur web et entrez l'adresse IP du serveur. La page Web du serveur doit être affichée.
      3. Établissez une connexion FTP entre **PC2** et **Serveur**. La connexion devrait échouer. Si ce n'est pas le cas, résolvez les instructions de liste d'accès et les configurations de groupe d'accès sur les interfaces.

Fermez la fenêtre de configuration.

Fin du document