Packet Tracer - Configurer les ACLs étendues - Scénario 1

Partie 1 : Configurer, appliquer et vérifier un ACL étendu numéroté

Étape 1 : Configurer un ACL pour permettre FTP et ICMP à partir du LAN du PC1.

Étape 1 : Configurer un ACL pour permettre FTP et ICMP à partir du LAN du PC1.

a. Depuis le mode de configuration globale sur **R1**, entrez la commande suivante pour déterminer le premier numéro valide pour une liste d'accès étendue.

```
R1(config)# access-list ?
<1-99> IP standard access list
<100-199> IP extended access list
```

b. Ajoutez **100** à la commande, suivi 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
```

c. Pour autoriser le trafic FTP, entrez **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
```

d. Lorsqu'elle est configurée et appliquée, cette ACL devrait permettre le FTP et l'ICMP. L'ICMP est mentionné ci-dessus, mais le FTP ne l'est pas. En effet, le FTP est un protocole de la couche application qui utilise le TCP au niveau de la couche 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
```

e. L'adresse source peut représenter un seul appareil, tel que PC1, en utilisant le mot-clé **host** puis l'adresse IP de PC1. L'utilisation du mot-clé **any** permet d'héberger 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
```

f. Calculer le masque de joker en déterminant l'opposé binaire du masque de sous-réseau /27.

```
11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.00011111 = 0.0.0.31
```

g. Saisissez le masque de remplacement, 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
```

h. 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
```

i. Notez que l'une des options est (retour chariot). En d'autres termes, vous pouvez appuyer sur la touche **Enter** et la déclaration permettra le trafic de tous les TCP. Cependant, nous n'autorisons que le trafic FTP ; par conséquent, entrez le mot-clé **eq** , suivi d'un point d'interrogation pour afficher les options disponibles. Ensuite, entrez **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
```

j. Créer une deuxième déclaration de liste d'accès pour permettre le trafic ICMP (ping, etc.) du PC1 au serveur. Notez que le numéro de la liste d'accès reste le même et qu'il n'est pas nécessaire de préciser le type de trafic ICMP.

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

Exécutez la commande **show access-list**et vérifiez que access list 100 contient les instructions correctes. Notez que l'instruction **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 de 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
```

Étape 2 : Appliquez l'ACL sur la bonne interface pour filtrer le trafic.

Du point de vue de **R1**, le trafic auquel s'applique l'ACL 100 provient du 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
```

Partie 2 : Configurer, appliquer et vérifier une liste ACL nommée étendue

Étape 1 : Configurer une liste ACL pour autoriser l'accès HTTP et ICMP à partir du réseau local PC2.

a. Les ACL nommées commencent par le mot-clé **ip**. Depuis le mode de configuration globale de **R1**, entrez la commande suivante, suivie d'un point d'interrogation.

```
R1(config)# ip access-list ?
extended Extended Access List
standard Standard Access List
```

b. Vous pouvez configurer des ACLs standard et étendues nommées. Cette liste d'accès filtre à la fois les adresses IP source et destination ; elle doit donc être étendue. Saisissez **HTTP_ONLY** comme nom. (Pour l'évaluation du traceur de paquets, 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
```

c. L'invite change. Vous êtes maintenant en mode de configuration étendu nommé ACL. Tous les appareils du réseau local **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
```

d. Une autre façon de calculer un joker consiste à 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
```

e. Terminez la déclaration 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 host172.22.34.62
eq www
```

f. Créer une deuxième déclaration de liste d'accès pour permettre le trafic ICMP (ping, etc.) de **PC2** vers le **serveur**. Remarque : l'invite reste la même et il n'est pas nécessaire de spécifier un type de trafic ICMP spécifique.

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

g. Tout autre trafic est refusé, par défaut. Sortie étendue nommée mode de configuration ACL

h. 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
```

Étape 2 : Appliquez l'ACL sur la bonne interface 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. Entrez dans le mode de configuration de l'interface et appliquez la ACL.

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

```
R1(config)# interface gigabitEthernet 0/1
R1(config-if)# ip access-group HTTP_ONLY in
```

Étape 3 : Vérifier la mise en œuvre de la ACL .

a. Ping du **PC2** vers le **serveur**. Si le ping est infructueux, vérifiez les adresses IP avant de continuer.

b. Depuis le PC2, ouvrez un navigateur web et entrez l'adresse IP du serveur. La page Web du serveur doit être affichée.

c. FTP du **PC2** au **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.