Packet Tracer : configuration des listes de contrôle d'accès étendues, scénario 1

Topologie

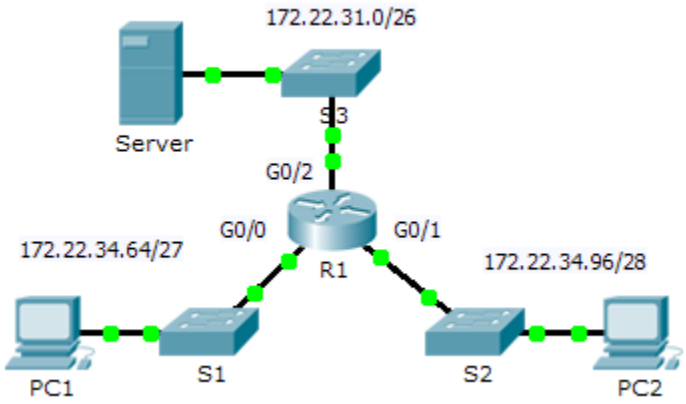

Table d'adressage

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

Objectifs

Partie 1 : configuration, application et vérification d'une liste de contrôle d'accès numérotée étendue

Partie 2 : configuration, application et vérification d'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.

Partie 1 : Configuration, application et vérification d'une liste de contrôle d'accès numérotée étendue

Étape 1 : Configurez une liste de contrôle d'accès pour autoriser l'accès FTP et ICMP.

a. 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.

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

b. 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
```

c. 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
```

d. Cette liste de contrôle d'accès autorise FTP et ICMP. ICMP est indiqué ci-dessus, mais FTP non car FTP utilise TCP. Vous devez donc spécifier TCP. Saisissez **tcp** pour affiner davantage l'aide de la liste de contrôle d'accès.

```
R1(config)# access-list 100 permit tcp ?
  A.B.C.D  Source address
  any      Any source host
  host     A single source host
```

e. Notez que nous pourrions garder juste **PC1** en utilisant le mot-clé **host**, ou autoriser tous les hôtes avec **any**. Dans ce cas, tout périphérique ayant une adresse appartenant au réseau 172.22.34.64/27 est autorisé. Tapez l'adresse 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. Calculez le masque générique déterminant l'inverse binaire d'un masque de sous-réseau.

11111111.11111111.11111111.11100000 = 255.255.255.224
00000000.00000000.00000000.000**11111** = 0.0.0.31

g. 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
```

h. Configurez l'adresse de destination. Dans ce scénario, nous filtrons le trafic pour une seule destination, le serveur. Tapez 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>
```

i. 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. En l'occurrence, nous autorisons uniquement le trafic FTP. Par conséquent, entrez le mot-clé **eq** suivi d'un point d'interrogation pour afficher les options disponibles. Ensuite, tapez **ftp** et appuyez sur **Entrée**.

```
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. Créez une deuxième instruction de liste d'accès pour autoriser le trafic ICMP (ping, etc.) entre **PC1** et **Server**. Notez que le numéro de la liste d'accès reste identique et qu'un type de trafic ICMP spécifique n'a pas besoin d'être spécifié.

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

k. Par défaut, tout autre trafic est refusé.

Étape 2 : 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 ACL 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.

```
R1(config)# interface gigabitEthernet 0/0
R1(config-if)# ip access-group 100 in
```

Étape 3 : Vérifiez l'implémentation de la liste de contrôle d'accès.

a. Envoyez une requête ping de **PC1** vers **Server**. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.

b. Établissez une connexion FTP entre **PC1** et **Server**. Le nom d'utilisateur et le mot de passe sont **cisco**.

```
PC> ftp 172.22.34.62
```

c. Quittez le service FTP de **Server**.

```
ftp> quit
```

d. Envoyez une requête ping de **PC1** vers **PC2**. L'hôte de destination doit être inaccessible, car le trafic n'est pas autorisé explicitement.

Partie 2 : Configuration, application et vérification d'une liste de contrôle d'accès nommée étendue

Étape 1 : Configurez une liste de contrôle d'accès pour autoriser l'accès HTTP et ICMP.

a. 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.

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

b. 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. Tapez **HTTP_ONLY** comme nom. (Pour la note Packet Tracer, le nom est sensible à la casse.)

```
R1(config)# ip access-list extended HTTP_ONLY
```

c. L'invite change. Vous êtes maintenant en mode de configuration de liste de contrôle d'accès nommée étendue. Tous les périphériques du LAN de **PC2** ont besoin d'un accès TCP. Tapez l'adresse 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 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 ?
```

e. 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
```

f. Créez une deuxième instruction de liste d'accès pour autoriser le trafic ICMP (ping, etc.) entre **PC2** et **Server**. 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
```

g. Par défaut, tout autre trafic est refusé. Quittez le mode de configuration de liste de contrôle d'accès nommée étendue.

Étape 2 : 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.

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

Étape 3 : Vérifiez l'implémentation de la liste de contrôle d'accès.

a. Envoyez une requête ping de **PC2** vers **Server**. Si les requêtes ping n'aboutissent pas, vérifiez les adresses IP avant de continuer.

b. Établissez une connexion FTP entre **PC2** et **Server**. La connexion doit échouer.

c. Ouvrez le navigateur Web sur **PC2** et entrez l'adresse IP de **Server** comme URL. La connexion devrait cette fois aboutir.