Travaux pratiques : dépannage de la configuration et du placement des listes de contrôle d'accès

Topologie

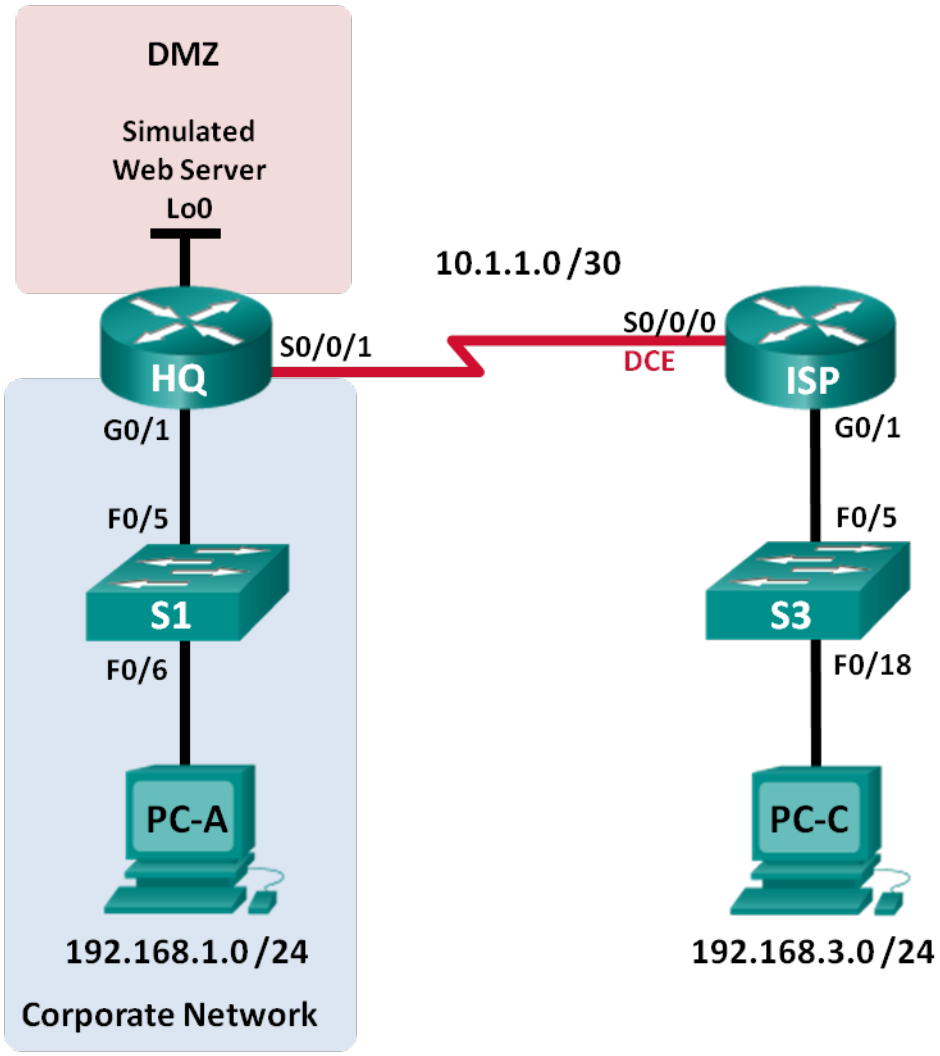

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
HQ	G0/1	192.168.1.1	255.255.255.0	N/A
	S0/0/1	10.1.1.2	255.255.255.252	N/A
	Lo0	192.168.4.1	255.255.255.0	N/A
ISP	G0/1	192.168.3.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
S3	VLAN 1	192.168.3.11	255.255.255.0	192.168.3.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1

Objectifs

Partie 1 : création du réseau et configuration des paramètres de périphérique de base

Partie 2 : dépannage de l'accès interne

Partie 3 : dépannage de l'accès distant

Contexte/scénario

Une liste de contrôle d'accès (ACL) est une série de commandes IOS permettant de filtrer le trafic de base sur un routeur Cisco. Les listes de contrôle d'accès sont utilisées pour sélectionner les types de trafic à traiter. Une instruction ACL unique est appelée « entrée de contrôle d'accès » (ACE). Ces entrées sont évaluées de haut en bas, avec l'instruction deny all implicite à la fin de la liste. Les listes de contrôle d'accès permettent également de contrôler les types de trafic entrant ou sortant d'un réseau par les hôtes source et de destination ou le réseau. Pour gérer correctement le trafic souhaité, le placement de la liste de contrôle d'accès est essentiel.

Dans ces travaux pratiques, une petite entreprise vient juste d'ajouter un serveur Web sur le réseau pour permettre aux clients d'accéder à des informations confidentielles. Le réseau d'entreprise est divisé en deux zones : la zone réseau d'entreprise et la zone démilitarisée (DMZ). La zone réseau d'entreprise héberge les serveurs privés et les clients internes. La DMZ héberge le serveur Web externe accessible depuis l'extérieur (simulé avec Lo0 sur HQ). Étant donné que la société peut gérer uniquement son propre routeur HQ, toutes les listes de contrôle d'accès doivent être appliquées au routeur HQ.

- La liste de contrôle d'accès ACL 101 est mise en œuvre pour limiter le trafic sortant de la zone réseau d'entreprise. Cette zone héberge les serveurs privés et les clients internes (192.168.1.0/24). Aucun autre réseau ne doit être en mesure d'y accéder.
- La liste de contrôle d'accès ACL 102 est utilisée pour limiter le trafic entrant sur le réseau d'entreprise. Seules les réponses aux requêtes provenant du réseau d'entreprise sont autorisées à revenir sur ce réseau. Cela comprend les requêtes basées sur TCP provenant d'hôtes internes tels que Web et FTP. Le protocole ICMP est autorisé sur le réseau à des fins de dépannage de sorte que les messages ICMP entrants générés en réponse aux requêtes ping peuvent être reçus par des hôtes internes.

- La liste de contrôle d'accès ACL 121 contrôle le trafic extérieur vers la DMZ et le réseau d'entreprise. Seul le trafic HTTP est autorisé sur le serveur Web DMZ (simulé avec Lo0 sur R1). Les autres types de trafics liés aux réseaux, tel que le trafic EIGRP, sont autorisés depuis les réseaux externes. En outre, des adresses privées internes valides, telles que 192.168.1.0, des adresses de bouclage telles que 127.0.0.0 et des adresses de multidiffusion se voient refuser l'entrée au réseau d'entreprise pour empêcher les attaques réseau malveillantes provenant d'utilisateurs externes.

Remarque : les routeurs utilisés lors des travaux pratiques CCNA sont des routeurs à services intégrés (ISR) Cisco 1941 équipés de Cisco IOS version 15.2(4)M3 (image universalk9). Les commutateurs utilisés sont des modèles Cisco Catalyst 2960s équipés de Cisco IOS version 15.0(2) (image lanbasek9). D'autres routeurs, commutateurs et versions de Cisco IOS peuvent être utilisés. Selon le modèle et la version de Cisco IOS, les commandes disponibles et le résultat produit peuvent varier de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau Résumé des interfaces du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration initiale. En cas de doute, contactez votre instructeur.

Ressources requises

- 2 routeurs (Cisco 1941 équipé de Cisco IOS version 15.2(4)M3 image universelle ou similaire)
- 2 commutateurs (Cisco 2960 équipés de Cisco IOS version 15.0(2) image lanbasek9 ou similaire)
- 2 PC (Windows 7, Vista ou XP, équipés d'un programme d'émulation du terminal tel que Tera Term)
- Câbles de console pour configurer les périphériques Cisco IOS via les ports de console
- Câbles Ethernet et série conformément à la topologie

Partie 1: Création du réseau et configuration des paramètres de base du périphérique

Dans la Partie 1, vous allez configurer la topologie du réseau ainsi que les routeurs et les commutateurs avec des paramètres de base, tels que des mots de passe et des adresses IP. Les configurations prédéfinies vous sont également fournies pour les configurations initiales du routeur. Vous configurerez également les paramètres IP pour les PC de la topologie.

Étape 1: Câblez le réseau conformément à la topologie.

Étape 2: Configurez les hôtes de PC.

Étape 3: Initialisez et redémarrez les routeurs et les commutateurs, le cas échéant.

Étape 4: (Facultatif) Configurez les paramètres de base pour chaque commutateur.

a. Désactivez la recherche DNS.

b. Configurez les noms d'hôtes conformément à la topologie.

c. Configurez l'adresse IP et la passerelle par défaut dans la table d'adressage.

d. Attribuez **cisco** comme mots de passe de console et vty.

e. Attribuez **class** comme mot de passe du mode d'exécution privilégié.

f. Configurez **logging synchronous** pour empêcher les messages de console d'interrompre la commande.

Étape 5: Configurez les paramètres de base pour chaque routeur.

a. Désactivez la recherche DNS.

b. Configurez les noms d'hôtes conformément à la topologie.

c. Attribuez **cisco** comme mots de passe de console et vty.

d. Attribuez **class** comme mot de passe du mode d'exécution privilégié.

e. Configurez **logging synchronous** pour empêcher les messages de console d'interrompre la commande.

Étape 6: Configurez les accès HTTP et les identifiants utilisateur sur le routeur HQ.

Les informations d'identification d'utilisateurs locaux sont configurées pour accéder au serveur Web simulé (192.168.4.1).

```
HQ(config)# ip http server
HQ(config)# username admin privilege 15 secret adminpass
HQ(config)# ip http authentication local
```

Étape 7: Chargez les configurations de routeur.

Les configurations des routeurs ISP et HQ vous sont fournies. Il existe des erreurs dans ces configurations, et votre rôle consiste à déterminer les configurations incorrectes et de les corriger.

Routeur ISP

```
hostname ISP
interface GigabitEthernet0/1
 ip address 192.168.3.1 255.255.255.0
 no shutdown
interface Serial0/0/0
 ip address 10.1.1.1 255.255.255.252
 clock rate 128000
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
 network 192.168.3.0
 no auto-summary
end
```

Routeur HQ

```
hostname HQ
interface Loopback0
 ip address 192.168.4.1 255.255.255.0
interface GigabitEthernet0/1
 ip address 192.168.1.1 255.255.255.0
 ip access-group 101 out
ip access-group 102 in
interface Serial0/0/1
 ip address 10.1.1.2 255.255.255.252
 ip access-group 121 in
 no shutdown
router eigrp 1
 network 10.1.1.0 0.0.0.3
```

```
 network 192.168.1.0
 network 192.168.4.0
 no auto-summary
access-list 101 permit ip 192.168.11.0 0.0.0.255 any
access-list 101 deny ip any any
access-list 102 permit tcp any any established
access-list 102 permit icmp any any echo-reply
access-list 102 permit icmp any any unreachable
access-list 102 deny ip any any
access-list 121 permit tcp any host 192.168.4.1 eq 89
access-list 121 deny icmp any host 192.168.4.11
access-list 121 deny ip 192.168.1.0 0.0.0.255 any
access-list 121 deny ip 127.0.0.0 0.255.255.255 any
access-list 121 deny ip 224.0.0.0 31.255.255.255 any
access-list 121 permit ip any any
access-list 121 deny ip any any
end
```

Partie 2: Résoudre les problèmes d'accès interne

Dans la Partie 2, les listes de contrôle d'accès sur le routeur HQ sont étudiées pour déterminer si elles sont configurées correctement.

Étape 1: Dépannez la liste de contrôle d'accès ACL 101

La liste de contrôle d'accès ACL 101 est mise en œuvre pour limiter le trafic sortant de la zone réseau d'entreprise. Cette zone héberge uniquement les clients internes et les serveurs privés. Seul le réseau 192.168.1.0/24 peut quitter cette zone réseau d'entreprise.

a. PC-A peut-il envoyer une requête ping à sa passerelle par défaut ?

b. Après avoir vérifié que PC-A a été configuré correctement, examinez le routeur HQ pour identifier d'éventuelles erreurs de configuration en affichant le récapitulatif de la liste de contrôle d'accès ACL 101. Entrez la commande **show access-lists 101**.

```
HQ# show access-lists 101
Extended IP access list 101
    10 permit ip 192.168.11.0 0.0.0.255 any
    20 deny ip any any
```

c. Est-ce qu'il y a des problèmes avec la liste de contrôle d'accès ACL 101 ?

d. Examinez l'interface de passerelle par défaut pour le réseau 192.168.1.0 /24. Vérifiez que la liste de contrôle d'accès ACL 101 est utilisée dans le sens correct sur l'interface G0/1. Tapez la commande **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  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
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 102
```

Le sens pour l'interface G0/1 est-il correctement configuré pour la liste de contrôle d'accès ACL 101 ?

e. Corrigez les erreurs concernant ACL 101 et vérifiez que le trafic provenant du réseau 192.168.1.0 /24 peut quitter le réseau d'entreprise. Notez les commandes utilisées pour corriger les erreurs.

f. Vérifiez que PC-A peut envoyer une requête ping à son interface de passerelle par défaut.

Étape 2: Dépannez la liste de contrôle d'accès ACL 102

La liste de contrôle d'accès ACL 102 est mise en œuvre pour limiter le trafic entrant sur le réseau d'entreprise. Le trafic provenant du réseau externe n'est pas autorisé sur le réseau d'entreprise. Le trafic distant est autorisé à entrer sur un réseau d'entreprise si le trafic établi provient du réseau interne. Les messages de réponse ICMP sont autorisés à des fins de dépannage.

a. PC-A peut-il envoyer une requête ping à PC-C ?

b. Examinez le routeur HQ pour identifier d'éventuelles erreurs de configuration en affichant le récapitulatif de la liste de contrôle d'accès ACL 102. Entrez la commande **show access-lists 102**.

```
HQ# show access-lists 102
Extended IP access list 102
    10 permit tcp any any established
    20 permit icmp any any echo-reply
    30 permit icmp any any unreachable
    40 deny ip any any (57 matches)
```

c. Est-ce qu'il y a des problèmes avec la liste de contrôle d'accès ACL 102 ?

d. Vérifiez que la liste de contrôle d'accès ACL 102 est utilisée dans le sens correct sur l'interface G0/1. Tapez la commande **show ip interface g0/1**.

```
HQ# show ip interface g0/1
GigabitEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.1/24
  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
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is 101
  Inbound  access list is 101
```

e. Est-ce qu'il y a des problèmes avec l'application de la liste de contrôle d'accès ACL 102 à l'interface G0/1 ?

f. Corrigez toutes les erreurs trouvées concernant la liste de contrôle d'accès ACL 102. Notez les commandes utilisées pour corriger les erreurs.

g. PC-A peut-il envoyer une requête ping à PC-C maintenant ?

Partie 3: Dépannage de l'accès distant

Dans la Partie 3, la liste de contrôle d'accès ACL 121 est configurée pour empêcher les attaques par mystification provenant des réseaux extérieurs et pour autoriser uniquement les accès HTTP distants au serveur Web (192.168.4.1) dans la DMZ.

a. Vérifiez que la liste de contrôle d'accès ACL 121 a été configurée correctement. Entrez la commande **show ip access-list 121**.

```
HQ# show ip access-lists 121
Extended IP access list 121
    10 permit tcp any host 192.168.4.1 eq 89
    20 deny icmp any host 192.168.4.11
    30 deny ip 192.168.1.0 0.0.0.255 any
    40 deny ip 127.0.0.0 0.255.255.255 any
    50 deny ip 224.0.0.0 31.255.255.255 any
    60 permit ip any any (354 matches)
    70 deny ip any any
```

Est-ce qu'il y a des problèmes avec cette liste de contrôle d'accès ?

b. Vérifiez que la liste de contrôle d'accès ACL 121 est utilisée dans le sens correct sur l'interface S0/0/1 de R1. Tapez la commande **show ip interface s0/0/1**.

```
HQ# show ip interface s0/0/1
Serial0/0/1 is up, line protocol is up
  Internet address is 10.1.1.2/30
  Broadcast address is 255.255.255.255
<Résultat omis>
  Multicast reserved groups joined: 224.0.0.10
  Outgoing access list is not set
  Inbound  access list is 121
```

Est-ce qu'il y a des problèmes avec l'application de cette liste de contrôle d'accès ?

c. Le cas échéant, si des erreurs se sont produites, effectuez et enregistrez les modifications de configuration nécessaires dans la liste de contrôle d'accès ACL 121.

d. Vérifiez que PC-C peut uniquement accéder au serveur Web simulé sur HQ à l'aide du navigateur Web. Fournissez le nom d'utilisateur **admin** et le mot de passe **adminpass** pour accéder au serveur Web (192.168.4.1).

Remarques générales

1. Dans quel ordre l'instruction ACL doit-elle figurer ? De général à spécifique ou inversement ?

2. Si vous supprimez une liste de contrôle d'accès à l'aide de la commande **no access-list** et qu'elle s'applique toujours à l'interface, que se passe-t-il ?

Tableau récapitulatif des interfaces de routeur

Résumé des interfaces de routeur				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Remarque : pour savoir comment le routeur est configuré, observez les interfaces afin d'identifier le type de routeur ainsi que le nombre d'interfaces qu'il comporte. Il n'est pas possible de répertorier de façon exhaustive toutes les combinaisons de configurations pour chaque type de routeur. Ce tableau inclut les identifiants des combinaisons possibles des interfaces Ethernet et série dans le périphérique. Ce tableau ne comporte aucun autre type d'interface, même si un routeur particulier peut en contenir un. L'exemple de l'interface RNIS BRI peut illustrer ceci. La chaîne de caractères entre parenthèses est l'abréviation normalisée qui permet de représenter l'interface dans les commandes de Cisco IOS.