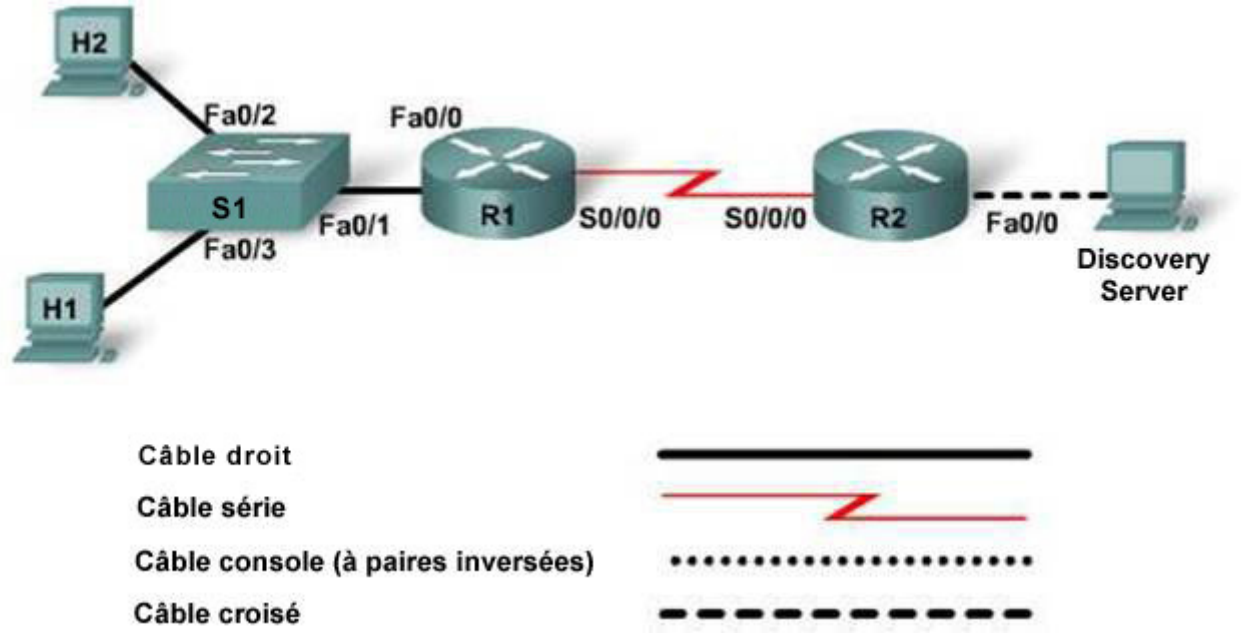
Travaux pratiques 8.5.1 : Configuration de listes de contrôle d'accès et vérification avec la journalisation de console



Périphérique	Nom de l'hôte	Adresse IP de l'interface FastEthernet 0/0	Adresse IP Serial 0/0/0	Type d'interface Serial 0/0/0	Instructions réseau	Mot de passe secret actif	Mot de passe enable/vty et console
Routeur 1	R1	192.168.1.1/24	192.168.5.1/30	DCE	192.168.1.0 192.168. 5.0	class	cisco
Routeur 2	R2	172.17.0.1/16	192.168.5.2/30	ETTD	192.168. 5.0 172.17.0.0	class	cisco
Commutateur 1	S1					class	cisco
Hôte 1	H1	192.168.1.5/24 Passerelle= 192.168.1.1					
Hôte 2	H2	192.168.1.6/24 Passerelle= 192.168.1.1					
Discovery Server	Server	172.17.1.1/16 Passerelle= 172.17.0.1					

Objectifs

- Configurer et vérifier des listes de contrôle d'accès pour contrôler le trafic
- Vérifier les listes de contrôle d'accès à l'aide des fonctions de journalisation du routeur

Contexte / Préparation

Installez un réseau similaire à celui du schéma de topologie. Tout routeur doté d'une interface indiquée dans le schéma ci-dessus peut être utilisé. Exemple : les routeurs de la gamme 800, 1600, 1700, 1800, 2500, 2600, 2800 ou toute combinaison de ces routeurs sont utilisables.

La syntaxe des commandes indiquée dans les travaux pratiques peut varier. Par exemple, les interfaces peuvent être différentes en fonction du modèle de routeur. Sur certains routeurs, Serial 0 peut être Serial 0/0 ou Serial 0/0/0 et Ethernet 0 peut être FastEthernet 0/0. Le commutateur Cisco Catalyst 2960 est fourni préconfiguré : il ne nécessite que l'affectation d'informations de sécurité de base avant la connexion à un réseau.

Ressources nécessaires :

- Un commutateur Cisco 2960 ou autre commutateur comparable
- Deux routeurs Cisco 1841 ou équivalents avec une connexion série et une interface Ethernet
- Deux PC Windows équipés d'un programme d'émulation de terminal et configurés comme hôtes
- Un PC devant jouer le rôle de Discovery Server
- Un CD Discovery Live pour le serveur
- Au moins un câble console à connecteur RJ-45/DB-9 pour configurer les routeurs et le commutateur
- Trois câbles droits Ethernet
- Un câble Ethernet croisé
- Un câble série ETTD/DCE

REMARQUE : vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. Les instructions d'effacement et de rechargement de la mémoire du commutateur et du routeur figurent dans la section Tools du site Academy Connection.

REMARQUE : Routeurs SDM – Si la configuration initiale (startup-config) est effacée dans un routeur SDM, le gestionnaire SDM ne s'affiche plus par défaut lorsque le routeur est redémarré. Il est alors nécessaire de définir une configuration de base de routeur à l'aide des commandes IOS. La procédure indiquée dans ces travaux pratiques utilise des commandes IOS et ne nécessite pas l'utilisation de SDM. Si vous voulez utiliser SDM, reportez-vous aux instructions du Manuel de travaux pratiques que vous pouvez télécharger depuis la section Tools du site Academy Connection. Consultez votre formateur si besoin.

REMARQUE : ces travaux pratiques utilisent le CD Discovery Server Live. Pour des instructions détaillées sur l'installation et la configuration du CD Discovery Server Live, consultez le manuel de travaux pratiques que vous pouvez télécharger depuis la section Tools du site Academy Connection.

Étape 1 : connexion du matériel

a. Connectez l'interface Serial 0/0/0 du routeur R1 à l'interface Serial 0/0/0 du routeur R2 à l'aide d'un câble série.

b. Connectez l'interface Fa0/0 du routeur R1 au port Fa0/1 du commutateur S1 à l'aide d'un câble droit.

c. Connectez l'hôte H1 au port Fa0/3 du Commutateur 1 à l'aide d'un câble droit.

d. Connectez l'hôte H2 au port Fa0/2 du Commutateur 1 à l'aide d'un câble droit.

e. Connectez le Discovery Server à l'interface Fa0/0 du routeur R2 à l'aide d'un câble croisé.

Étape 2 : configuration de base du routeur R1

Étape 3 : configuration de base du routeur R2

Étape 4 : configuration de base du commutateur S1

Étape 5 : configuration correcte des hôtes avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut

a. Configurez correctement chaque hôte avec l'adresse IP, le masque de sous-réseau et la passerelle par défaut.

   1) L'hôte H1 doit être configuré avec les paramètres suivants : adresse IP/masque de sous-réseau 192.168.1.5 /24 et passerelle par défaut 192.168.1.1.

   2) L'hôte H2 doit être configuré avec les paramètres suivants : adresse IP/masque de sous-réseau 192.168.1.6 /24 et passerelle par défaut 192.168.1.1.

   3) Le serveur doit être configuré avec les paramètres suivants : adresse IP 172.17.1.1 et passerelle par défaut 172.17.0.1.

b. Chaque hôte doit pouvoir envoyer une requête ping aux autres hôtes. Si cette requête échoue, procédez au dépannage requis. Vérifiez soigneusement qu'une adresse IP spécifique et une passerelle par défaut ont été attribuées à la station de travail. Ne configurez pas de listes de contrôle d'accès tant que chaque hôte ne peut pas envoyer de requête ping aux autres hôtes.

Étape 6 : configuration et application des listes de contrôle d'accès

Les listes de contrôle d'accès sont configurées pour contrôler les services auxquels les hôtes 1 et 2 peuvent accéder sur le serveur. La liste de contrôle d'accès créée permet l'accès Web (HTTP) et FTP de l'hôte H1 au serveur mais le refuse à l'hôte H2. Celui-ci sera autorisé à accéder au serveur par une connexion telnet, mais ce service sera interdit à l'hôte H1. Ces listes de contrôle d'accès seront configurées et vérifiées par des commandes **show** et la journalisation.

a. Créez une liste de contrôle d'accès conforme aux conditions ci-dessus. Cette liste de contrôle d'accès s'applique à R1.

```
R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any
```

b. Appliquez la liste de contrôle d'accès à l'interface FastEthernet 0/0 de R1 dans le sens entrant.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 110 in
```

c. Sur l'hôte H1, ouvrez un navigateur Web et essayez de vous connecter aux services Web et FTP du serveur. Dans la zone d'adresse du navigateur Web, entrez **http://172.17.1.1**.

   La connexion Web de l'hôte H1 a-t-elle abouti ? _____

d. Dans la zone d'adresse du navigateur Web, entrez **ftp://172.17.1.1**.

   La connexion FTP de l'hôte H1 a-t-elle abouti ? _____

e. Essayez de vous connecter aux services Web et FTP du serveur à partir de l'hôte H2.

   Pouvez-vous vous connecter à partir de l'hôte H2 ? _____

f. Essayez d'établir une connexion telnet au serveur à partir des Hôtes 1 et 2.

La connexion telnet de l'hôte H1 a-t-elle abouti ? _____

La connexion telnet de l'hôte H2 a-t-elle abouti ? _____

g. Utilisez la commande **show access-lists** pour afficher la liste de contrôle d'accès et les statistiques associées.

Quelles informations peuvent être tirées du résultat de la commande ?

_____

```
R1#show access-lists
Extended IP access list 110
    10 permit tcp host 192.168.1.5 host 172.17.1.1 eq www (3 matches)
    20 permit tcp host 192.168.1.5 host 172.17.1.1 eq ftp (9 matches)
    30 permit tcp host 192.168.1.6 host 172.17.1.1 eq telnet (3 matches)
    40 deny ip any any (92 matches)
```

Le résultat de la commande **show access-lists** affiche le nombre de correspondances renvoyées par chaque ligne `access-list`. Dans de nombreux scénarios de dépannage, cependant, ces informations ne sont pas suffisantes. Ainsi, le résultat affiché ci-dessus indique que la ligne **deny ip any any** a obtenu 92 correspondances. Mais cela n'indique pas quel type de trafic a été envoyé et à partir de quelles sources il a été refusé. Si une liste de contrôle d'accès comporte une erreur qui empêche le trafic depuis ou vers une destination qu'elle n'était pas censée bloquer, des informations supplémentaires sont nécessaires. C'est dans ce type d'environnement que la journalisation peut s'avérer utile.

La même liste de contrôle d'accès va être configurée sur R1, mais cette fois-ci l'option de journalisation sera activée.

REMARQUE : activer l'option de journalisation d'une liste de contrôle d'accès équivaut à utiliser une commande **debug**. Dans un réseau de production, cette option peut imposer une charge importante aux ressources du routeur et ralentir le réseau, voire provoquer une panne. C'est pourquoi cette fonction doit être utilisée avec précaution dans un réseau de production.

h. Supprimez la liste de contrôle d'accès sur R1 et recréez-la avec l'option de journalisation.

```
R1(config)#no access-list 110

R1(config)#access-list 110 remark Allow Host 1 web access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq www log
R1(config)#access-list 110 remark Allow Host 1 FTP access to server
R1(config)#access-list 110 permit tcp host 192.168.1.5 host 172.17.1.1
eq ftp log
R1(config)#access-list 110 remark Allow Host 2 Telnet access to server
R1(config)#access-list 110 permit tcp host 192.168.1.6 host 172.17.1.1
eq telnet log
R1(config)#access-list 110 remark Deny all other traffic
R1(config)#access-list 110 deny ip any any log
```

i. Essayez d'établir une connexion telnet de l'hôte H1 au serveur.

Après avoir vérifié que l'hôte H1 ne parvient pas à établir la connexion, affichez le résultat à partir de la connexion console sur R1. Le résultat doit être similaire à celui-ci :

```
*Oct 18 01:10:570,466: %SEC-6-IPACCESSLOGP: list 110 denied tcp
192.168.1.5(1097) -> 172.17.1.1(23), 1 packet
```

La ligne affichée résulte de l'ajout de l'option **log** à une ligne `access-list`. Elle indique une date et une heure (`01:10:57.466`), le processus qui a généré le message de console (`%SEC-6-IPACCESSLOGP`) et des informations détaillées sur ce message (`list 110 denied tcp 192.168.1.5(1097) -> 172.17.1.1(23), 1 packet`).

Dans cet exemple, l'option de journalisation indique qu'une ligne access-list a renvoyé une correspondance et identifie également la source et la destination exactes du paquet correspondant.

j. Essayez d'envoyer une requête ping et d'utiliser des connexions Telnet, Web et FTP à partir des Hôtes 1 et 2 vers le Discovery Server.

Un message de journalisation est-il créé à chaque tentative de connexion ? _____

Les messages de console indiquent-ils les paquets autorisés par la liste de contrôle d'accès ainsi que ceux qui sont refusés ? _____

Si vous tentez d'établir des connexions très rapidement, un message semblable au suivant peut apparaître :

```
*Oct 18 01:26:39.638: %SEC-6-IPACCESSLOGRL: access-list logging rate-
limited or missed 1 packet
```

Ce message indique que le système IOS a détecté soit que le débit était trop élevé, soit que la console était trop occupée pour traiter tous les paquets. Dans cet exemple, il indique que le système a manqué un paquet. Pour éviter cette situation dans un réseau de production, limitez le nombre de lignes `access-list` pour lesquelles la journalisation est activée.

Étape 7 : remarques générales

a. Citez l'un des avantages que présente l'utilisation de l'option de journalisation dans une liste de contrôle d'accès par rapport aux informations fournies par la commande **show access-lists** ?

_____

b. Quel est le principal problème posé par l'activation de la fonction de journalisation d'une liste de contrôle d'accès ?

_____

c. En principe, activeriez-vous la journalisation pour plusieurs lignes ? Justifiez votre réponse.

_____

d. Si le réseau ne fonctionne pas comme prévu (par exemple, les mises à jour de routage ne sont pas effectuées, la résolution de noms n'a pas lieu), quelle instruction de liste de contrôle d'accès journaliseriez-vous ? _____