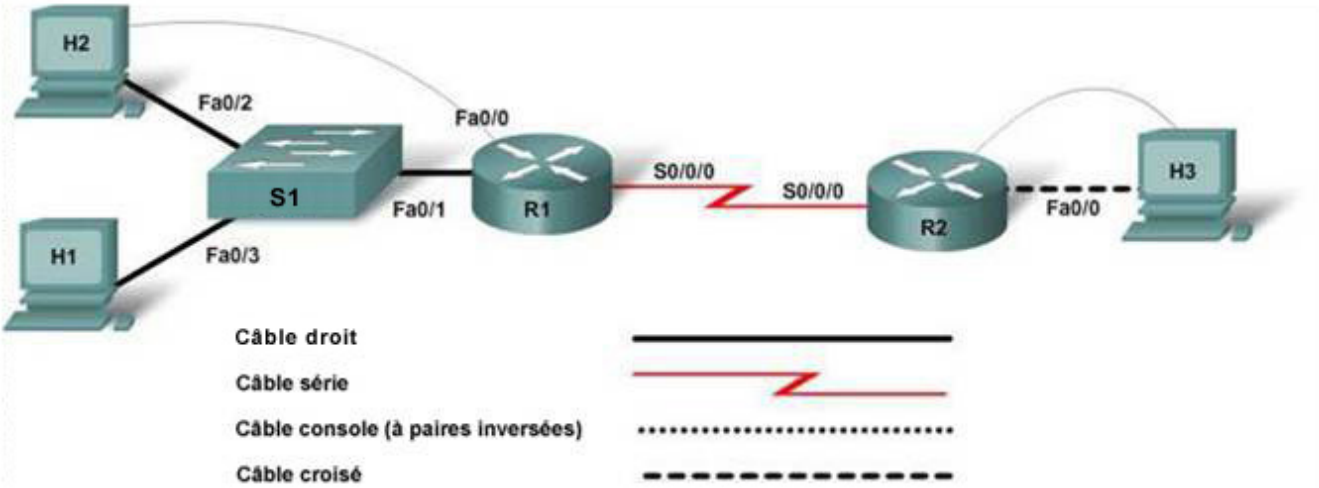
Travaux pratiques 8.3.4 : Planification, configuration et vérification de listes de contrôle d'accès étendues



Périphérique	Nom d'hôte	Adresse IP FastEthernet 0/0	Adresse IP Serial 0/0/0	Type d'interface Serial 0/0/0	Passerelle par défaut	Mot de passe secret actif	Mot de passe actif, vty et de console
Routeur 1	R1	192.168.1.1/24	192.168.15.1/30	DCE		class	cisco
Routeur 2	R2	192.168.5.1/24	192.168.15.2/30	ETTD		class	cisco
Commutateur 1	S1					class	cisco
Hôte 1	H1	192.168.1.10/24			192.168.1.1		
Hôte 2	H2	192.168.1.11/24			192.168.1.1		
Hôte 3	H3	192.168.5.10/24			192.168.5.1		

Objectifs

- Configurer des listes de contrôle d'accès étendues pour contrôler le trafic
- Vérifier le fonctionnement des listes de contrôle d'accès

Contexte / Préparation

Au cours de ces travaux pratiques, vous allez travailler avec des listes de contrôle d'accès étendues pour contrôler le trafic réseau sur la base d'adresses IP hôtes. Tout routeur doté d'une interface indiquée dans le schéma de topologie peut être utilisé. Exemple : les routeurs de la gamme 800, 1600, 1700, 1800, 2500, 2600, 2800 ou toute combinaison de ces routeurs sont utilisables.

Les informations présentées dans ces travaux pratiques s'appliquent aux routeurs de la gamme 1841. Elles s'appliquent aussi à d'autres routeurs ; cependant la syntaxe des commandes peut varier. Les interfaces peuvent être différentes en fonction du modèle de routeur. Par exemple, sur certains routeurs, Serial 0 peut être Serial 0/0 ou Serial 0/0/0 et Ethernet0 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 requises :

- Un commutateur Cisco 2960 ou autre commutateur comparable
- Deux routeurs Cisco 1841 ou équivalents, chacun avec une interface série et Ethernet
- Trois PC Windows, dont au moins un équipé d'un programme d'émulation de terminal, et tous configurés comme hôtes
- Au moins un câble console à connecteur RJ-45/DB-9 pour configurer les routeurs et le commutateur
- Trois câbles droits Ethernet
- Un câble croisé Ethernet
- Un câble croisé série ETTD/DCE en 2 parties

REMARQUE : assurez-vous que les routeurs et commutateurs ont été réinitialisés et ne possèdent aucune configuration de démarrage. 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.

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 à l'interface Fa0/1 du commutateur S1 à l'aide d'un câble droit.

c. Connectez un câble console à chaque PC pour procéder aux configurations sur les routeurs et le commutateur.

d. Connectez H1 au port Fa0/3 du commutateur S1 à l'aide d'un câble droit.

e. Connectez H2 au port Fa0/2 du commutateur S1 à l'aide d'un câble droit.

f. Connectez un câble croisé entre l'hôte H3 et l'interface Fa0/0 du routeur R2.

Étape 2 : configuration de base du routeur R1

a. Connectez un PC au port console du routeur pour procéder aux configurations à l'aide d'un programme d'émulation de terminal.

b. Sur le routeur R 1, configurez le nom d'hôte, les interfaces, les mots de passe et la bannière du message du jour, et désactivez les recherches DNS conformément à la table d'adressage et au schéma de topologie. Enregistrez la configuration.

Étape 3 : configuration de base du routeur R2

Procédez à la configuration de base du routeur R2 et enregistrez-la.

Étape 4 : configuration de base du commutateur S1

Configurez le commutateur S1 avec un nom d'hôte et des mots de passe de console, Telnet et privilégié, selon la table d'adressage et le schéma de topologie.

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

a. Configurez les hôtes avec une adresse IP, un masque de sous-réseau et une passerelle par défaut, conformément à la table d'adressage et au schéma de topologie.

b. Chaque station de travail doit pouvoir envoyer un paquet ping au routeur auquel elle est connectée. Si les requêtes ping échouent, procédez au dépannage requis. Vérifiez soigneusement qu'une adresse IP spécifique et une passerelle par défaut ont été attribuées à la station de travail.

Étape 6 : configuration du routage RIP et vérification de la connectivité de bout en bout dans le réseau

a. Sur R1, activez le protocole de routage RIP et configurez-le de façon à annoncer les deux réseaux connectés.

b. Sur R2, activez le protocole de routage RIP et configurez-le de façon à annoncer les deux réseaux connectés.

c. Envoyez une requête ping depuis chaque hôte vers les deux autres hôtes.

La requête ping a-t-elle abouti ? _____

Si la réponse est non, vérifiez la configuration de l'hôte et du routeur pour trouver l'erreur. Envoyez de nouvelles requêtes ping jusqu'à ce qu'elles aboutissent toutes.

Étape 7 : configuration des listes de contrôle d'accès étendues pour contrôler le trafic

L'hôte H3 de ce réseau contient des informations propriétaires. Les exigences du réseau en matière de sécurité imposent que l'accès à cette machine ne soit accordé qu'à certains périphériques. L'hôte H1 est le seul qui sera autorisé à accéder à cet ordinateur. Tous les autres hôtes de ce réseau sont utilisés pour un accès de type invité (guest) et ne doivent pas être autorisés à accéder à l'hôte H3. En outre, l'hôte H3 est le seul ordinateur du réseau qui soit autorisé à accéder aux interfaces R1 pour la gestion à distance. Des listes de contrôle d'accès étendues vont être utilisées pour contrôler l'accès à ce réseau.

a. Pour plus de clarté, dressez la liste des conditions requises :

1) L'hôte H1 peut accéder à l'hôte H3. Aucun autre hôte (sur ce réseau uniquement) ne peut accéder à l'hôte H3. Les hôtes supplémentaires ajoutés par la suite sur d'autres réseaux devraient être en mesure d'accéder à l'hôte H3 parce que ce ne seront pas des machines accessibles par invité.

2) L'hôte H3 peut accéder aux interfaces R1. Aucun autre périphérique du réseau ne disposera d'un accès.

b. Analysez les conditions requises et déterminez l'emplacement des listes de contrôle d'accès étendues.

Selon les conditions requises, le trafic à contrôler est celui qui part de l'interface Fa0/0 de R2 à destination de l'hôte H3. Par conséquent, la liste de contrôle d'accès doit être placée sur l'interface Fa0/0 de R2.

c. Créez une liste de contrôle d'accès étendue pour effectuer les tâches indiquées et appliquez-la à R2.

```
R2(config)#access-list 101 permit ip host 192.168.1.10 host
192.168.5.10
R2(config)#access-list 101 deny ip 192.168.1.0 0.0.0.255 host
192.168.5.10
R2(config)#access-list 101 permit ip any any
R2(config)#access-list 101 deny ip any any
```

REMARQUE : l'instruction **deny** implicite à la fin d'une liste de contrôle d'accès remplit la même fonction. Cependant, il est recommandé d'ajouter la ligne à la fin de la liste afin d'en conserver une trace. Lorsque cette instruction est ajoutée explicitement, le nombre de paquets correspondant à l'instruction est compté, ce qui permet à l'administrateur de savoir combien de paquets ont été refusés.

d. Appliquez la liste de contrôle d'accès sur l'interface Fa0/0 de R2 dans le sens des sorties.

```
R2(config)#interface fastethernet 0/0
R2(config-if)#ip access-group 101 out
```

e. Vérifiez la liste de contrôle d'accès sur R2 à l'aide de la commande **show access-lists**.

Le résultat de la commande **show access-lists** indique-t-il la liste de contrôle d'accès qui a été créée ?

_____

Le résultat de la commande **show access-lists** indique-t-il comment la liste de contrôle d'accès est appliquée ?

_____

f. Utilisez la commande **show ip interface fa0/0** sur R2 pour afficher l'application de la liste de contrôle d'accès.

Que vous indique le résultat de la commande **show ip interface** sur la liste de contrôle d'accès ?

_____

Étape 8 : test de la liste de contrôle d'accès

a. Envoyez une requête ping à H3 à partir des hôtes H1 et H2.

H1 peut-il envoyer une requête ping à H3 ? _____

H2 peut-il envoyer une requête ping à H3 ? _____

b. Pour vérifier que d'autres adresses peuvent envoyer une requête ping à H3, envoyez une requête ping à H3 à partir de R1.

La requête ping a-t-elle abouti ? _____

c. Affichez de nouveau la liste de contrôle d'accès à l'aide de la commande **show access-lists**.

Quelles autres informations sont affichées en dehors des instructions de la liste de contrôle d'accès ?

_____

d. Supprimez cette liste de contrôle d'accès avant de poursuivre.

```
R2(config)#interface fastethernet 0/0
R2(config-if)#no ip access-group 101 out
R2(config-if)#exit
R2(config)#no access-list 101
```

Étape 9 : configuration et test de la liste de contrôle d'accès pour la condition suivante

a. H3 est le seul hôte qui doit être autorisé à se connecter à R1 pour la gestion à distance. Créez une liste de contrôle d'accès pour répondre à cette condition. Cette liste devra être placée sur R1 parce que ce dernier est la destination du trafic. L'accès ne sera autorisé à aucun autre hôte. C'est le seul trafic qui est contrôlé ; tout autre trafic doit être autorisé.

```
R1(config)#access-list 101 permit ip host 192.168.5.10 host
192.168.15.1
R1(config)#access-list 101 permit ip host 192.168.5.10 host 192.168.1.1
R1(config)#access-list 101 deny ip any host 192.168.15.1
R1(config)#access-list 101 deny ip any host 192.168.1.1
R1(config)#access-list 101 permit ip any any
R1(config)#access-list 101 deny ip any any
```

b. Comme le trafic source peut provenir de n'importe quelle direction, cette liste de contrôle d'accès doit être appliquée aux deux interfaces de R1. Le trafic à contrôler est le trafic entrant dans le routeur.

```
R1(config)#interface fastethernet 0/0
R1(config-if)#ip access-group 101 in
R1(config-if)#interface serial 0/0/0
R1(config-if)#ip access-group 101 in
```

c. Essayez maintenant d'établir une connexion Telnet à R1 à partir de tous les hôtes et de R2. Tentez d'établir une connexion Telnet aux deux adresses de R1.

Pouvez-vous établir une connexion Telnet à partir de ces périphériques ? Si oui, lequel ou lesquels ?

_____

d. Affichez le résultat de la commande **show access-lists** sur R1.

Le résultat de la commande **show access-lists** indique-t-il des correspondances avec les instructions ? _____

Étape 10 : remarques générales

a. Pourquoi est-il nécessaire de procéder à une planification et à des tests minutieux des listes de contrôle d'accès ?

_____

b. Citez l'un des avantages de l'utilisation de listes de contrôle d'accès étendues par rapport aux listes standard ?

_____