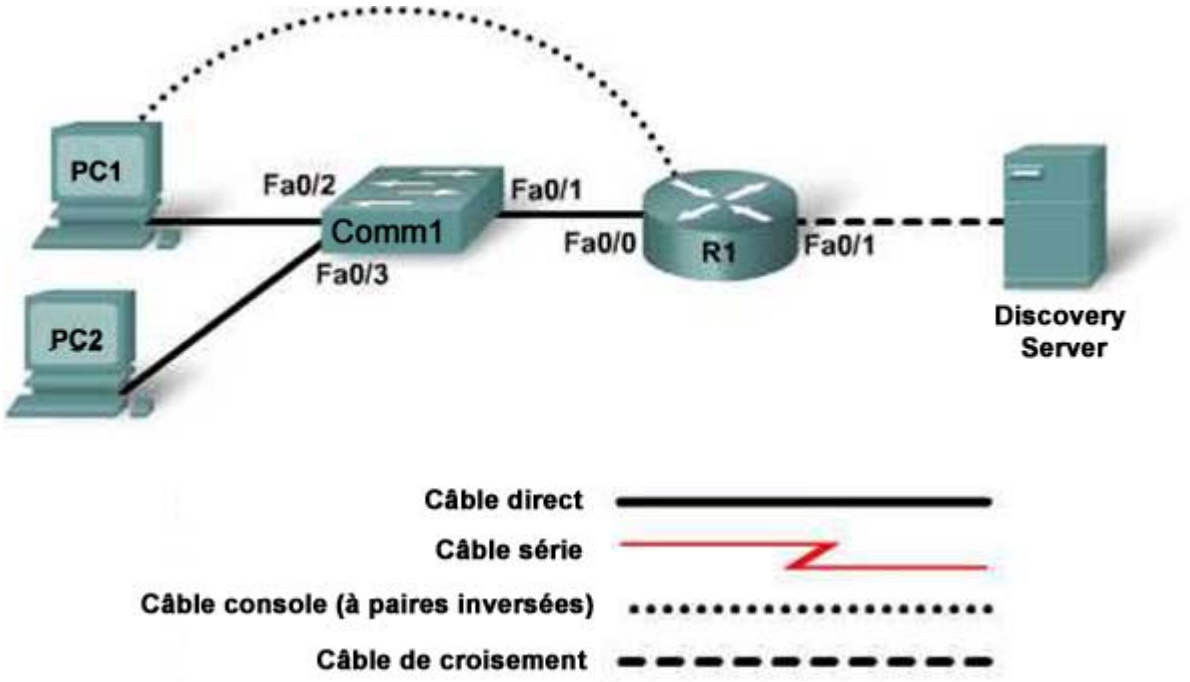
Travaux pratiques 1.3.4 Création d'une liste de contrôle d'accès



Périphérique	Nom d'hôte	Adresse	Masque de sous-réseau
Discovery Server	Serveur	172.17.1.1	255.255.0.0
R1	FC-CPE-1	Fa0/1 172.17.0.1 Fa0/0 10.0.0.1	255.255.0.0 255.255.255.0
Comm1	FC-ASW-1	—	—
Hôte1	PC1	10.0.0.10	255.255.255.0
Hôte2	PC2	10.0.0.201	255.255.255.0

Objectif

- Créer des listes de contrôle d'accès pour filtrer le trafic à des fins de sécurité et de gestion du trafic

Objectifs de l'examen CCNA 640-802

Ces travaux pratiques font appel à des compétences qui se rapportent aux objectifs d'examen CCNA suivants :

- Configurer et appliquer des listes de contrôle d'accès d'après les exigences de filtrage du réseau (y compris ILC/SDM)
- Configurer et appliquer des listes de contrôle d'accès afin de restreindre l'accès Telnet et SSH au routeur (notamment SDM et l'ICL)
- Vérifier et surveiller les listes de contrôle d'accès dans un environnement de réseau

Résultats attendus et critères de réussite

Avant de commencer ces travaux pratiques, lisez les tâches que vous devez effectuer. Selon vous, quel sera le résultat de l'exécution de ces tâches ?

_____

_____

_____

En quoi est-il utile d'avoir une compréhension des listes de contrôle d'accès en administration réseau ?

_____

_____

_____

Comment un administrateur réseau sait-il si la liste de contrôle d'accès fonctionne correctement ?

_____

_____

_____

Contexte / Préparation

Au cours de ces travaux pratiques, vous allez examiner la nécessité de contrôler et de filtrer le trafic des données dans un réseau, et concevrez les politiques à ces fins.

La conception de la sécurité du trafic sera ensuite appliquée à un réseau utilisant les listes de contrôle d'accès.

Celles-ci sont généralement appliquées dans la couche de distribution. Ces travaux pratiques utilisent un routeur connecté à un serveur fournissant des applications réseau afin d'illustrer le positionnement et le fonctionnement des listes de contrôle d'accès.

Étape 1 : analyse des besoins de filtrage du trafic

a. Déterminez les besoins d'accès et de filtrage.

Pour ces travaux pratiques :

1) PC1 désigne la station de travail de l'administrateur réseau. Cet hôte doit posséder l'accès FTP et HTTP au serveur du réseau et l'accès Telnet au routeur FC-CPE-1.

2) PC2 désigne une station de travail possédant uniquement un accès HTTP. Les services FTP et l'accès Telnet au routeur ne sont pas autorisés.

b. Après avoir déterminé les besoins spécifiques, décidez si le trafic restant est autorisé ou refusé.

Dressez la liste des avantages et des problèmes éventuels pour les scénarios de filtrage suivants :

Avantages à autoriser le trafic restant :

_____

Problèmes éventuels liés à l'autorisation du trafic restant :

_____

Avantages à refuser le trafic restant :

_____

Problèmes éventuels liés au refus du trafic restant :

_____

Étape 2 : conception et création de la liste de contrôle d'accès

a. Passez en revue puis appliquez les pratiques recommandées concernant les listes de contrôle d'accès.

- Planifiez toujours soigneusement avant la mise en œuvre.
- L'ordre des instructions est important. Placez les instructions spécifiques au début et les plus générales à la fin.
- Les instructions sont ajoutées à la fin de la liste de contrôle au fur et à mesure de leur écriture.
- Créez et modifiez les listes de contrôle d'accès au moyen d'un éditeur de texte et enregistrez le fichier.
- Utilisez les listes de contrôle d'accès nommées autant qu'il est possible.
- Employez les commentaires (option **`remark`**) dans la liste de contrôle pour décrire à quoi servent les instructions.
- Les listes de contrôle d'accès doivent être appliquées à une interface pour entrer en vigueur.
- Une interface ne peut comporter qu'une seule liste de contrôle d'accès par protocole de couche réseau et par direction.
- Bien qu'une instruction **deny any** est implicite à la fin de chaque liste de contrôle, il est de bon usage de la rendre explicite. Ainsi, vous vous souvenez qu'elle est en vigueur et vous pouvez utiliser la journalisation de ces instructions.
- Le traitement des listes de contrôle d'accès comprenant de nombreuses instructions est plus long et peut avoir de l'influence sur les performances du routeur.
- Emplacement des listes de contrôle d'accès :
    - Standard : le plus près possible de la destination (si vous possédez l'autorité d'administration sur le routeur) ;
    - Étendues : le plus près possible de la source (si vous possédez l'autorité d'administration sur le routeur).

b. Prenez en considération les deux méthodes d'écriture des listes de contrôle d'accès :

- Autoriser d'abord le trafic spécifique puis refuser le trafic général.
- Refuser d'abord le trafic spécifique puis autoriser le trafic général.

Quand est-il préférable d'autoriser d'abord le trafic spécifique puis de refuser le trafic général ?

_____

_____

Quand est-il préférable de refuser d'abord le trafic spécifique puis d'autoriser le trafic général ?

_____

_____

c. Sélectionnez une méthode et écrivez les instructions de liste de contrôle d'accès selon le but de ces travaux pratiques.

_____

_____

_____

_____

_____

_____

Après l'écriture d'une liste de contrôle d'accès et son application à une interface, il est bon de savoir si les instructions ont l'effet escompté. Le nombre de paquets répondant aux conditions de chaque instruction de la liste peut être journalisé en ajoutant l'option **log** à la fin de l'instruction.

Pourquoi est-il important de savoir combien de fois les paquets correspondant à une instruction de la liste sont refusés ?

_____

_____

Étape 3 : câblage et configuration du réseau donné

REMARQUE : si les PC utilisés dans ces travaux pratiques sont également connectés au réseau local de votre établissement ou à Internet, assurez-vous de bien noter les raccordements de câbles et les paramètres TCP/IP afin que ceux-ci puissent être rétablis à la fin des travaux pratiques.

a. En vous référant au schéma de la topologie, connectez le câble console (à paires inversées) au port console du routeur et l'autre extrémité au port COM1 de l'ordinateur hôte à l'aide d'un adaptateur DB-9 ou DB-25. Assurez-vous que l'ordinateur hôte et le routeur sont tous les deux sous tension.

b. Connectez et configurez les périphériques selon la topologie et la configuration fournies. Votre formateur peut remplacer Discovery Server par un serveur équivalent.

c. Établissez une émulation de terminal HyperTerminal (ou autre) de PC1 au routeur R1.

d. À partir du mode de configuration globale, entrez les commandes suivantes :

```
Router(config)#hostname FC-CPE-1

FC-CPE-1(config)#interface FastEthernet0/0
FC-CPE-1(config-if)#ip address 10.0.0.1 255.255.255.0
FC-CPE-1(config-if)#no shutdown
FC-CPE-1(config-if)#exit

FC-CPE-1(config)#interface FastEthernet0/1
FC-CPE-1(config-if)#ip address 172.17.0.1 255.255.0.0
FC-CPE-1(config-if)#no shutdown
FC-CPE-1(config-if)#exit

FC-CPE-1(config)#line vty 0 4
```

```
FC-CPE-1(config-line)#password telnet
FC-CPE-1(config-line)#login
FC-CPE-1(config-line)#end
```

e. Envoyez une requête ping du PC1 au Discovery Server pour vérifier la connectivité du réseau. Si la requête ping échoue, effectuez le dépannage puis établissez la connectivité.

Étape 4 : test des services de réseau sans liste de contrôle d'accès

Effectuez les tests suivants sur PC1 :

a. Ouvrez un navigateur Web sur PC1 et saisissez l'URL **http://172.17.1.1** dans la barre d'adresse.

Quelle est la page Web affichée ?

_____

b. Ouvrez un navigateur Web sur PC1 et saisissez l'URL **ftp://172.17.1.1** dans la barre d'adresse.

Quelle est la page Web affichée ?

_____

c. Dans le répertoire de base de Discovery FTP, ouvrez le dossier **Discovery 1**. Cliquez sur le fichier d'un chapitre et faites-le glisser sur le bureau local.

Le fichier a-t-il été correctement copié ? _____

d. À l'invite de ligne de commande de PC1, lancez la commande **`telnet 10.0.0.1`** ou utilisez un client Telnet (par exemple HyperTerminal ou TeraTerm) pour ouvrir une session Telnet sur le routeur.

Quelle est la réponse affichée par le routeur ?

_____

e. Quittez la session Telnet.

Effectuez les tests suivants sur PC2 :

a. Ouvrez un navigateur Web sur PC2 et saisissez l'URL **http://172.17.1.1** dans la barre d'adresse.
Quelle est la page Web affichée ?

_____

b. Ouvrez un navigateur Web sur PC2 et saisissez l'URL **ftp://172.17.1.1** dans la barre d'adresse.
Quelle est la page Web affichée ?

_____

c. Dans le répertoire de base de Discovery FTP, ouvrez le dossier **Discovery 1**. Cliquez sur le fichier d'un chapitre et faites-le glisser sur le bureau local.
Le fichier a-t-il été correctement copié ? _____

d. À l'invite de ligne de commande de PC2, lancez la commande **`telnet 10.0.0.1`** ou utilisez un client Telnet (par exemple HyperTerminal ou TeraTerm) pour ouvrir une session Telnet sur le routeur.
Quelle est la réponse affichée par le routeur ?

_____

e. Quittez la session Telnet.

Pourquoi les deux connexions ci-dessus se sont-elles déroulées avec succès ?

_____

_____

Si la ou les connexions ci-dessus ont échoué, procédez au dépannage du réseau et des configurations puis établissez les deux types de connexion à partir de chaque hôte.

Étape 5 : configuration de la liste de contrôle d'accès des services de réseau

À partir du mode de configuration globale, entrez les commandes suivantes :

a. Autorisez PC1 à accéder au serveur Web et à établir une connexion Telnet vers le routeur.

```
FC-CPE-1(config)#ip access-list extended Server-Access
FC-CPE-1(config-ext-nacl)#remark Autoriser PC1 à accéder au serveur
FC-CPE-1(config-ext-nacl)#permit tcp host 10.0.0.10 host 172.17.1.1 eq
ftp www log
```

b. Autorisez PC2 à accéder au serveur Web.

```
FC-CPE-1(config-ext-nacl)#remark Autoriser PC2 à accéder au serveur Web
FC-CPE-1(config-ext-nacl)#permit tcp host 10.0.0.201 host 172.17.1.1 eq
www log
```

c. Autorisez l'accès Telnet de PC1 au routeur.

FC-CPE-1(config-ext-nacl)#**remark Autoriser PC1 à établir une connexion Telnet au routeur**

FC-CPE-1(config-ext-nacl)#permit tcp host 10.0.0.10 host 10.0.0.1 eq telnet log

d. Refusez tout autre trafic.

```
FC-CPE-1(config-ext-nacl)#remark Refuser tout autre trafic
FC-CPE-1(config-ext-nacl)#deny ip any any log
FC-CPE-1(config-ext-nacl)#exit
```

Étape 6 : application des listes de contrôle d'accès

a. Appliquez la liste de contrôle d'accès étendue à l'interface du routeur la plus proche de la source.

```
FC-CPE-1(config)#interface FastEthernet0/0
FC-CPE-1(config-if)#ip access-group Server-Access in
FC-CPE-1(config-if)#end
```

b. Dans le mode d'exécution privilégié, lancez la commande **show running-configuration** puis confirmez les bonnes configuration et application des listes de contrôle d'accès.

Reconfigurez-les si vous trouvez des erreurs.

Étape 7 : test des services de réseau avec listes de contrôle d'accès

Effectuez les tests suivants sur PC1 :

a. Ouvrez un navigateur Web sur PC1 et saisissez l'URL **http://172.17.1.1** dans la barre d'adresse.

Quelle est la page Web affichée ?

_____

b. Ouvrez un navigateur Web sur PC1 et saisissez l'URL **ftp://172.17.1.1** dans la barre d'adresse.

Quelle est la page Web affichée ?

_____

c. Dans le répertoire de base de Discovery FTP, ouvrez le dossier **Discovery 1**. Cliquez sur le fichier d'un chapitre et faites-le glisser sur le bureau local.

Le fichier a-t-il été correctement copié ? _____

Pourquoi ce résultat ?

_____

d. À l'invite de ligne de commande de PC1, lancez la commande **`telnet 10.0.0.1`** ou utilisez un client Telnet (par exemple HyperTerminal ou TeraTerm) pour ouvrir une session Telnet sur le routeur.

Quelle est la réponse affichée par le routeur ?

_____

Pourquoi ce résultat ?

_____

e. Quittez la session Telnet.

Effectuez les tests suivants sur PC2 :

a. Ouvrez un navigateur Web sur PC2 et saisissez l'URL **http://172.17.1.1** dans la barre d'adresse.

Quelle est la page Web affichée ?

_____

Pourquoi ce résultat ?

_____

b. Ouvrez un navigateur Web sur PC2 et saisissez l'URL **ftp://172.17.1.1** dans la barre d'adresse.

Quelle est la page Web affichée ?

_____

Pourquoi ce résultat ?

_____

c. À l'invite de ligne de commande de PC2, lancez la commande **`telnet 10.0.0.1`** ou utilisez un client Telnet (par exemple HyperTerminal ou TeraTerm) pour ouvrir une session Telnet sur le routeur.

Quelle est la réponse affichée par le routeur ?

_____

Pourquoi ce résultat ?

_____

Si la ou les transactions n'ont pas donné le résultat attendu, procédez au dépannage du réseau et des configurations et testez à nouveau les listes de contrôle d'accès à partir de chaque hôte.

Étape 8 : observation du nombre de correspondances d'instructions

a. En mode d'exécution privilégié, entrez la commande :

```
FC-CPE-1#show access-list Server-Access
```

Énumérez les correspondances journalisées pour chaque instruction de la liste de contrôle d'accès.

_____

_____

Étape 9 : remise en état

Effacez les configurations et redémarrez les routeurs et commutateurs. Déconnectez et rangez le câblage. Pour les PC hôtes habituellement connectés à d'autres réseaux (comme le réseau local de l'établissement ou Internet), reconnectez le câblage approprié et restaurez les paramètres TCP/IP.

Confirmation

Réécrivez la liste de contrôle d'accès au serveur utilisé dans ces travaux pratiques de façon à ce que :

1) les stations de travail administrateur soient considérées comme étant comprises dans la plage d'adresses 10.0.0.10 /24 à 10.0.0.15 /24 au lieu d'un seul hôte ;
2) les stations de travail normales soient comprises dans la plage d'adresses 10.0.0.16 /24 à 10.0.0.254 /24 au lieu d'un seul hôte.

_____

_____

_____

_____

_____

_____

_____