Travaux pratiques : configuration et vérification des restrictions VTY

Topologie

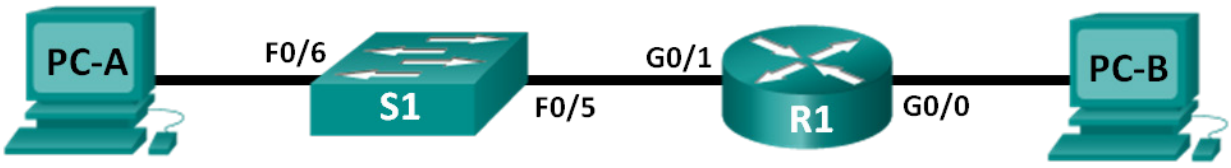

Table d'adressage

Appareil	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/0	192.168.0.1	255.255.255.0	N/A
	G0/1	192.168.1.1	255.255.255.0	N/A
S1	VLAN 1	192.168.1.2	255.255.255.0	192.168.1.1
PC-A	Carte réseau	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	Carte réseau	192.168.0.3	255.255.255.0	192.168.0.1

Objectifs

Partie 1 : Configurer les paramètres de base des périphériques

Partie 2 : configuration et application de la liste de contrôle d'accès sur R1

Partie 3 : vérification de la liste de contrôle d'accès via Telnet

Partie 4 : défi : configuration et application de la liste de contrôle d'accès sur S1

Contexte/scénario

Il est recommandé de limiter l'accès aux interfaces d'administration de routeurs, comme la console et les lignes vty. Une liste de contrôle d'accès (ACL) peut être utilisé pour autoriser l'accès d'adresses IP spécifiques, ce qui garantit que seuls les ordinateurs d'administrateur sont autorisés à accéder via Telnet ou SSH au routeur.

Remarque : Dans les sorties des périphériques Cisco, la liste de contrôle d'accès est abrégée en liste d'accès.

Au cours de ces travaux pratiques, vous allez créer et appliquer une liste de contrôle d'accès standard nommée pour limiter l'accès distant aux lignes vty du routeur.

Après avoir créé et appliqué la liste de contrôle d'accès, vous la testerez et vérifierez en accédant au routeur à partir de différentes adresses IP via Telnet.

Ces travaux pratiques fournissent les commandes nécessaires à la création et l'application de la liste de contrôle d'accès.

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 2960 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 différer de ceux indiqués dans les travaux pratiques. Reportez-vous au tableau récapitulatif de l'interface du routeur à la fin de ces travaux pratiques pour obtenir les identifiants d'interface corrects.

Remarque : vérifiez que la mémoire des routeurs et des commutateurs a été effacée et qu'aucune configuration de démarrage n'est présente. En cas de doute, contactez votre formateur.

Ressources requises

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

Remarque : les interfaces Gigabit Ethernet des routeurs Cisco 1941 sont à détection automatique et un câble Ethernet droit peut être utilisé entre le routeur et PC-B. Si vous utilisez un autre modèle de routeur Cisco, un câble Ethernet croisé pourrait être nécessaire.

Partie 1 : Configurer les paramètres de base des périphériques

Dans la Partie 1, vous allez configurer la topologie du réseau et configurer les adresses IP des interfaces, l'accès des périphériques et les mots de passe sur le routeur.

Étape 1 : Connectez le réseau conformément au schéma de topologie indiqué.

Étape 2 : Configurez les paramètres réseau de PC-A et PC-B conformément à la table d'adressage.

Étape 3 : Initialisez et redémarrez le routeur et le commutateur.

a. Accédez au routeur par la console et passez en mode de configuration globale.

b. Copiez la configuration de base suivante et collez-la dans la configuration en cours sur le routeur.

```
no ip domain-lookup
hostname R1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (Accès sans autorisation
strictement interdit.) #
Line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. Configurez les adresses IP sur les interfaces répertoriées dans la table d'adressage.

d. Enregistrez la configuration en cours dans le fichier de configuration initiale.

e. Accédez au commutateur par la console et passez en mode de configuration globale.

f. Copiez la configuration de base suivante et collez-la dans la configuration en cours sur le commutateur.

```
no ip domain-lookup
hostname S1
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. (Accès sans autorisation
strictement interdit.) #
Line con 0
password cisco
login
logging synchronous
line vty 0 15
password cisco
login
exit
```

g. Configurez une adresse IP sur l'interface VLAN1 répertoriée dans la table d'adressage.

h. Configurez la passerelle par défaut pour le commutateur.

i. Enregistrez la configuration en cours dans le fichier de configuration initiale.

Partie 2 : Configuration et application de la liste de contrôle d'accès sur R1

Dans la Partie 2, vous allez configurer une liste de contrôle d'accès standard nommée et l'appliquer aux lignes de terminal virtuel de routeur pour restreindre les accès à distance au routeur.

Étape 1 : Configurez et appliquez une liste de contrôle d'accès nommée standard.

a. Accédez au routeur R1 par la console et activez le mode d'exécution privilégié.

b. À partir du mode de configuration globale, affichez les options de commande sous **ip access-list** à l'aide d'un espace et d'un point d'interrogation.

```
R1(config)# ip access-list ?
  extended    liste d'accès étendue
  helper      actions de la liste d'accès sur la commande helper-address
  log-update  contrôle des mises à jour du journal de la liste d'accès
  logging     contrôle de la connexion à la liste d'accès
  resequence  remise en ordre de la liste d'accès
  standard    liste d'accès standard
```

c. Affichez les options de commande sous **ip access-list standard** à l'aide d'un espace et d'un point d'interrogation.

```
R1(config)# ip access-list standard ?
  <1-99>       numéro de la liste d'accès IP standard
  <1300-1999>  numéro de la liste d'accès IP standard (plage étendue)
  WORD         nom de la liste d'accès
```

d. Ajoutez **ADMIN-MGT** à la fin de la commande **ip access-list standard** et appuyez sur Entrée. Vous êtes maintenant en mode de configuration de liste d'accès nommée standard (config-std-nacl).

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)#
```

e. Entrez votre entrée de contrôle d'accès d'autorisation ou d'interdiction de liste de contrôle d'accès, également connue sous le nom d'instruction ACL, une ligne à la fois. N'oubliez qu'il y a une instruction **deny any** implicite à la fin de la liste de contrôle d'accès, interdisant effectivement tout trafic. Entrez un point d'interrogation pour afficher les options de la commande.

```
R1(config-std-nacl)# ?
Commandes de configuration de la liste d'accès standard :
  <1-2147483647>  numéro de série
  default         restauration des configurations par défaut d'une commande
  deny            instruction pour le rejet des paquets
  exit            quitter le mode de configuration de liste d'accès
  no              annuler une commande ou restaurer ses paramètres par défaut
  permit            instruction pour la transmission des paquets
  remark          commentaire sur les entrées de la liste d'accès
```

f. Créez une ACE d'autorisation pour PC-A administrateur à l'adresse 192.168.1.3 et une ACE d'autorisation supplémentaire afin de permettre l'accès des autres adresses IP réservées aux périphériques administrateurs, de 192.168.1.4 à 192.168.1.7. Notez pourquoi la première entrée ACE d'autorisation indique un hôte unique en utilisant le mot de passe **host**. Il aurait été préférable d'utiliser l'entrée ACE **permit 192.168.1.3 0.0.0.0**. La deuxième entrée de contrôle d'accès permit autorise les hôtes 192.168.1.4 à 192.168.1.7, en utilisant le masque générique 0.0.0.3, qui est l'inverse d'un masque de sous-réseau 255.255.255.252.

```
R1(config-std-nacl)# permit host 192.168.1.3
R1(config-std-nacl)# permit 192.168.1.4 0.0.0.3
R1(config-std-nacl)# exit
```

Il n'est pas nécessaire de saisir une entrée de contrôle d'accès deny car il existe une entrée de contrôle d'accès **deny all** implicite à la fin de la liste de contrôle d'accès.

g. Maintenant que l'entrée de contrôle d'accès nommée est créée, appliquez-la aux lignes vty.

```
R1(config)# line vty 0 15
R1(config-line)# access-class ADMIN-MGT in
R1(config-line)# exit
```

Partie 3 : Vérification de la liste de contrôle d'accès via Telnet

Dans la Partie 3, vous allez utiliser Telnet pour accéder au routeur et vérifier que la liste de contrôle d'accès nommée fonctionne correctement.

Remarque : le protocole SSH est mieux sécurisé que Telnet ; cependant, SSH nécessite que le périphérique réseau soit configuré pour accepter les connexions SSH. Telnet est utilisé dans ces travaux pratiques par souci de facilité.

a. Ouvrez une invite de commande sur PC-A et vérifiez que vous pouvez communiquer avec le routeur en exécutant une commande **ping**.

```
C:\Users\user1> ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
```

```
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64
Reply from 192.168.1.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 5ms, Average = 2ms
C:\Users\user1>
```

b. À partir de l'invite de commande sur PC-A, lancez le programme client Telnet pour établir une connexion Telnet avec le routeur. Saisissez votre identifiant et les mots de passe actifs. Vous devriez être connecté avec succès, voir le message de bannière et recevoir une invite de commande du routeur R1.

```
C:\Users\user1> telnet 192.168.1.1

L'accès non autorisé est interdit !

Contrôle de l'accès de l'utilisateur

Password:
R1>actif
Password:
R1#
```

La connexion Telnet a-t-elle abouti ? _____

c. Tapez **exit** à l'invite de commande et appuyez sur Entrée pour quitter la session Telnet.

d. Modifiez votre adresse IP pour vérifier si la liste de contrôle d'accès nommée bloque les adresses IP non autorisées. Remplacez l'adresse IPv4 par 192.168.1.100 sur PC-A.

e. Essayez à nouveau d'établir une connexion Telnet avec R1 sur 192.168.1.1. La session Telnet a-t-elle abouti ?

_____

Quel message a-t-il été reçu ? _____

f. Modifiez l'adresse IP sur PC-A pour vérifier si la liste de contrôle d'accès nommée autorise un hôte dont l'adresse IP figure dans la plage 192.168.1.4 - 192.168.1.7 à établir une connexion Telnet avec le routeur. Après avoir modifié l'adresse IP sur PC-A, ouvrez une invite de commande Windows et essayez d'établir une connexion Telnet avec le routeur R1.

La session Telnet a-t-elle abouti ?

_____

_____

g. À partir du mode d'exécution privilégié sur R1, tapez la commande **show ip access-lists** et appuyez sur Entrée. Dans le résultat de la commande, notez que Cisco IOS affecte automatiquement les numéros de ligne aux entrées de contrôle d'accès (ACE) de la liste de contrôle d'accès (ACL) par incréments de 10 et indique le nombre de fois que chaque entrée de contrôle d'accès d'autorisation (permit) a été correctement associée (entre parenthèses).

```
# show ip route
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
```

Puisque deux connexions Telnet ont été correctement établies avec le routeur et que chaque session Telnet a été lancée à partir d'une adresse IP correspondant à l'une des entrées de contrôle d'accès permit, il y a des correspondances pour chaque entrée de contrôle d'accès permit.

À votre avis, pourquoi est-ce qu'il y a deux correspondances pour chaque entrée de contrôle d'accès permit alors qu'une seule connexion a été lancée à partir de chaque adresse IP ?

_____

_____

_____

_____

Comment pouvez-vous déterminer à quel stade le protocole Telnet génère les deux correspondances lors de la connexion Telnet ?

_____

_____

_____

h. Sur R1, accédez au mode de configuration globale.

i. Passez en mode de configuration de liste d'accès pour la liste d'accès nommée ADMIN-MGT et ajoutez une entrée de contrôle d'accès **deny any** à la fin de la liste d'accès.

```
R1(config)# ip access-list standard ADMIN-MGT
R1(config-std-nacl)# deny any
R1(config-std-nacl)# exit
```

Remarque : Étant donné qu'une entrée ACE **deny any** implicite se trouve à la fin de toutes les listes de contrôle d'accès, ajouter une entrée ACE **deny any** explicite n'est pas nécessaire. Cependant, la condition « deny any » explicite à la fin des listes de contrôle d'accès peut toujours être utilisée par l'administrateur réseau pour se connecter ou simplement pour connaître le nombre de correspondances des ACE de liste d'accès **deny any**.

j. Essayez d'établir une connexion Telnet à partir de PC-B vers R1. Ceci crée une correspondance avec l'entrée de contrôle d'accès **deny any** dans la liste d'accès nommée ADMIN-MGT.

k. À partir du mode d'exécution privilégié, tapez la commande **show ip access-lists** et appuyez sur Entrée. Vous devriez maintenant voir plusieurs correspondances avec l'entrée de contrôle d'accès **deny any**.

```
# show ip route
Standard IP access list ADMIN-MGT
    10 permit 192.168.1.3 (2 matches)
    20 permit 192.168.1.4, wildcard bits 0.0.0.3 (2 matches)
    30 deny any (3 matches)
```

La connexion Telnet défectueuse génère plus de correspondances avec l'entrée de contrôle d'accès deny explicite qu'une connexion ayant abouti. Pourquoi ?

_____

_____

Partie 4 : Défi : configuration et application de la liste de contrôle d'accès sur S1

Étape 1 : Configurez et appliquez une liste de contrôle d'accès standard nommée pour les lignes vty sur S1.

a. Sans vous reporter aux commandes de configuration de R1, essayez de configurer la liste de contrôle d'accès sur S1, en autorisant uniquement l'adresse IP de PC-A.

b. Appliquez la liste de contrôle d'accès aux lignes vty de S1. N'oubliez pas qu'il y a plus de lignes vty sur un commutateur qu'un routeur.

Étape 2 : Testez la liste de contrôle d'accès vty sur S1.

Établissez une connexion Telnet à partir de chacun des PC pour vérifier que la liste de contrôle d'accès vty fonctionne correctement. Vous devriez pouvoir établir une connexion Telnet à S1 à partir de PC-A, mais pas à partir de PC-B.

Remarques générales

1. Comme le démontre l'accès vty distant, les listes de contrôle d'accès sont de puissants filtres de contenu pouvant être appliqués à d'autres éléments que simplement des interfaces réseau entrantes et sortantes. Quelles sont les autres méthodes d'application des listes de contrôle d'accès ?

   _____

   _____

2. Une liste de contrôle d'accès appliquée à une interface de gestion à distance vty permet-elle d'améliorer la sécurité de la connexion Telnet ? Est-ce que cela fait de Telnet un outil de gestion d'accès distant plus durable?

   _____

   _____

   _____

3. Pourquoi est-il utile d'appliquer une liste de contrôle d'accès à des lignes vty plutôt qu'à des interfaces spécifiques ?

   _____

   _____

   _____

Tableau récapitulatif des interfaces des routeurs

Résumé des interfaces des routeurs				
Modèle du routeur	**Interface Ethernet 1**	**Interface Ethernet 2**	**Interface série 1**	**Interface série 2**
1 800	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 différentes combinaisons d'interfaces Ethernet et série possibles 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 Cisco IOS.