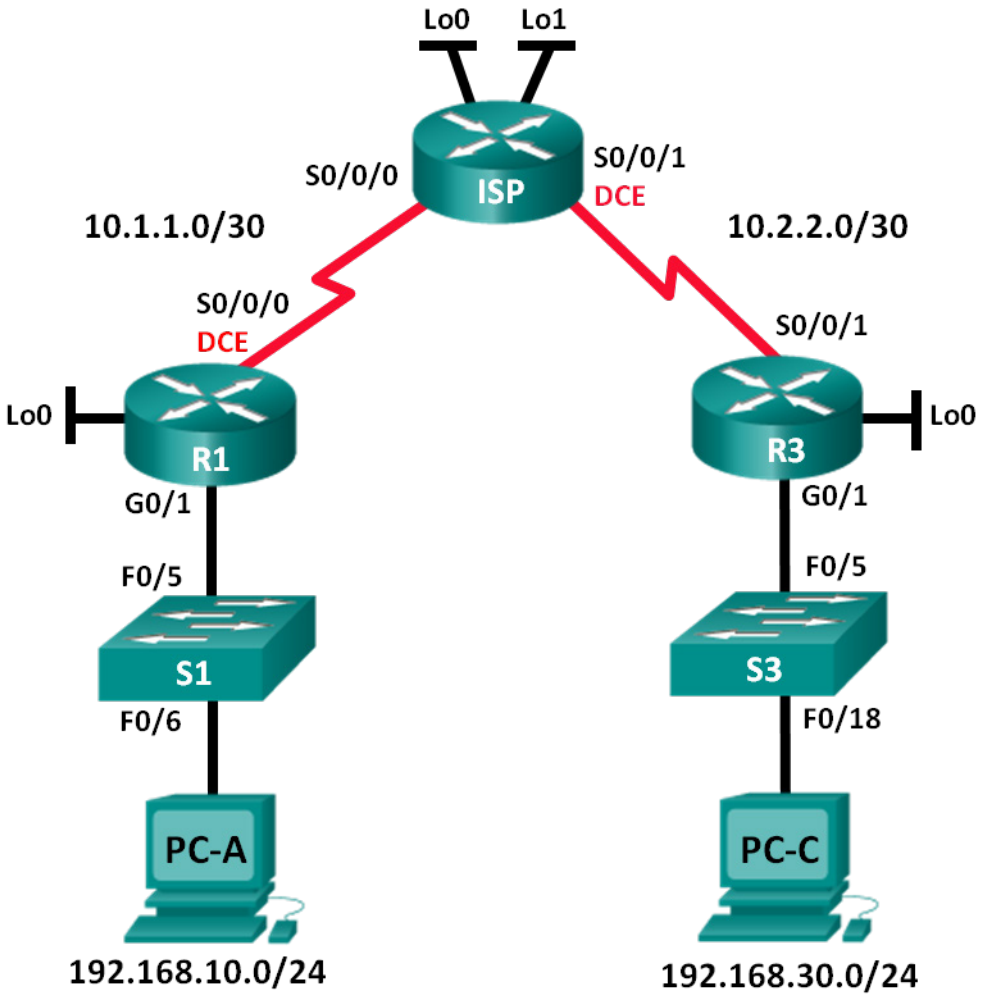
Travaux pratiques : configuration et vérification des listes de contrôle d'accès étendues

Topologie



© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Table d'adressage

Périphérique	Interface	Adresse IP	Masque de sous-réseau	Passerelle par défaut
R1	G0/1	192.168.10.1	255.255.255.0	N/A
	Lo0	192.168.20.1	255.255.255.0	N/A
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	N/A
ISP	S0/0/0	10.1.1.2	255.255.255.252	N/A
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	N/A
	Lo0	209.165.200.225	255.255.255.224	N/A
	Lo1	209.165.201.1	255.255.255.224	N/A
R3	G0/1	192.168.30.1	255.255.255.0	N/A
	Lo0	192.168.40.1	255.255.255.0	N/A
	S0/0/1	10.2.2.1	255.255.255.252	N/A
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S3	VLAN 1	192.168.30.11	255.255.255.0	192.168.30.1
PC-A	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	192.168.30.3	255.255.255.0	192.168.30.1

Objectifs

Partie 1 : configuration de la topologie et initialisation des périphériques

Partie 2 : configuration des périphériques et vérification de la connectivité

- Configuration des paramètres de base sur des ordinateurs, des routeurs et des commutateurs.
- Configurez le routage EIGRP sur R1, ISP et R3.

Partie 3 : configuration et vérification des listes de contrôle d'accès numérotées et nommées étendues

- Configurez, appliquez et vérifiez une liste de contrôle d'accès étendue numérotée.
- Configurez, appliquez et vérifiez une liste de contrôle d'accès nommée numérotée.

Partie 4 : modification et vérification des listes de contrôle d'accès étendues

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Contexte/scénario

Les listes de contrôle d'accès (ACL) étendues sont extrêmement puissantes. Elles offrent un niveau de contrôle beaucoup plus important que les listes de contrôle d'accès standard en ce qui concerne les types de trafic pouvant être filtrés, ainsi que l'origine et la destination du trafic.

Dans ces travaux pratiques, vous allez configurer le filtrage des règles pour deux bureaux représentés par R1 et R3. La direction a établi certaines stratégies d'accès entre les LAN situés au niveau de R1 et R3, que vous devez implémenter. Le routeur ISP entre R1 et R3 ne comporte aucune liste de contrôle d'accès. Aucun accès administratif ne serait octroyé à un routeur ISP étant donné que vous pouvez uniquement contrôler et gérer votre propre matériel.

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

- 3 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: Configuration de la topologie et initialisation des périphériques

Dans la Partie 1, vous allez configurer la topologie du réseau et effacer toutes les configurations, le cas échéant.

Étape 1: Câblez le réseau conformément à la topologie.

Étape 2: Initialisez et redémarrez les routeurs et les commutateurs.

Partie 2: Configuration des périphériques et vérification de la connectivité

Dans la Partie 2, vous configurerez les paramètres de base sur les routeurs, les commutateurs et les ordinateurs. Reportez-vous à la topologie et à la table d'adressage pour le nom des périphériques et les informations d'adressage.

Étape 1: Configurez les adresses IP sur PC-A et PC-C.

Étape 2: Configurez les paramètres de base sur R1.

a. Désactivez la recherche DNS.

b. Configurez le nom du périphérique conformément à la topologie.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

c. Créez une interface de bouclage sur R1.

d. Configurez les adresses IP d'interface conformément à la topologie et à la table d'adressage.

e. Configurez un mot de passe **class** pour le mode d'exécution privilégié.

f. Attribuez une fréquence d'horloge de **128000** à l'interface S0/0/0.

g. Attribuez **cisco** comme mot de passe pour la console et vty et activez l'accès Telnet. Configurez **logging synchronous** pour les lignes de console et vty.

h. Autorisez l'accès Web sur R1 pour simuler un serveur Web avec une authentification locale pour l'utilisateur **admin**.

```
R1(config)# ip http server
R1(config)# ip http authentication local
R1(config)# username admin privilege 15 secret class
```

Étape 3: Configurez les paramètres de base sur ISP.

a. Configurez le nom du périphérique conformément à la topologie.

b. Créez les interfaces de bouclage sur le routeur ISP.

c. Configurez les adresses IP d'interface conformément à la topologie et à la table d'adressage.

d. Désactivez la recherche DNS.

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

f. Attribuez une fréquence d'horloge de **128000** à l'interface S0/0/1.

g. Attribuez **cisco** comme mot de passe pour la console et vty et activez l'accès Telnet. Configurez **logging synchronous** pour les lignes de console et vty.

h. Activez l'accès Web sur le routeur ISP. Utilisez les mêmes paramètres qu'à l'Étape 2h.

Étape 4: Configurez les paramètres de base sur R3.

a. Configurez le nom du périphérique conformément à la topologie.

b. Créez une interface de bouclage sur R3.

c. Configurez les adresses IP d'interface conformément à la topologie et à la table d'adressage.

d. Désactivez la recherche DNS.

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

f. Attribuez **cisco** comme mot de passe de console et configurez **logging synchronous** sur la ligne de console.

g. Activez SSH sur R3.

```
R3(config)# ip domain-name cisco.com
R3(config)# crypto key generate rsa modulus 1024
R3(config)# line vty 0 4
R3(config-line)# login local
R3(config-line)# transport input ssh
```

h. Activez l'accès Web sur R3. Utilisez les mêmes paramètres qu'à l'Étape 2h.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Étape 5: (Facultatif) Configurez les paramètres de base sur S1 et S3.

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

b. Configurez les adresses IP de l'interface de gestion conformément à la topologie et à la table d'adressage.

c. Désactivez la recherche DNS.

d. Configurez un mot de passe **class** pour le mode d'exécution privilégié.

e. Configurez une adresse de passerelle par défaut.

Étape 6: Configurez le routage EIGRP sur R1, ISP et R3.

a. Configurez le système autonome (AS) numéro 10 et annoncez tous les réseaux sur R1, ISP et R3. Désactivez la fonction de récapitulation automatique.

b. Après avoir configuré EIGRP sur R1, ISP et R3, vérifiez que tous les routeurs ont des tables de routage complètes indiquant tous les réseaux. Dépannez si ce n'est pas le cas.

Étape 7: Vérifiez la connectivité entre les périphériques.

Remarque : il est très important de vérifier la connectivité **avant** de configurer et mettre en application des listes de contrôle d'accès ! Assurez-vous que votre réseau fonctionne correctement avant de commencer à filtrer le trafic.

a. À partir de PC-A, envoyez une requête ping à PC-C et les interfaces série sur R3.

Les requêtes ping ont-elles abouti ?

b. À partir de R1, envoyez une requête ping à PC-C et l'interface série sur R3.

Les requêtes ping ont-elles abouti ?

c. À partir de PC-C, envoyez une requête ping à PC-A ainsi que l'interface série et de bouclage sur R1.

Les requêtes ping ont-elles abouti ?

d. À partir de R3, envoyez une requête ping à PC-A ainsi que l'interface de bouclage et série sur R1.

Les requêtes ping ont-elles abouti ?

e. À partir de PC-A, envoyez une requête ping aux interfaces de bouclage du routeur ISP.

Les requêtes ping ont-elles abouti ?

f. À partir de PC-C, envoyez une requête ping aux interfaces de bouclage du routeur ISP.

Les requêtes ping ont-elles abouti ?

g. Ouvrez un navigateur Web sur PC-A et accédez à http://209.165.200.225 sur le routeur ISP. Un nom d'utilisateur et un mot de passe vous sont demandés. Utilisez **admin** comme nom d'utilisateur et **class** comme mot de passe. Si vous êtes invité à accepter une signature, acceptez-la. Le routeur charge Cisco Configuration Professional (CCP) Express dans une fenêtre séparée. Vous serez peut-être invité à renseigner un nom d'utilisateur et un mot de passe. Utilisez **admin** comme nom d'utilisateur et **class** comme mot de passe.

h. Ouvrez un navigateur Web sur PC-C et accédez à http://10.1.1.1 sur R1. Un nom d'utilisateur et un mot de passe vous sont demandés. Utilisez **admin** comme nom d'utilisateur et **class** comme mot de passe. Si vous êtes invité à accepter une signature, acceptez-la. Le routeur charge CCP Express dans une fenêtre séparée. Vous serez peut-être invité à renseigner un nom d'utilisateur et un mot de passe. Utilisez **admin** comme nom d'utilisateur et **class** comme mot de passe.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Partie 3: Configuration et vérification des listes de contrôle d'accès numérotées et nommées étendues

Les listes de contrôle d'accès étendues permettent de filtrer le trafic de plusieurs façons. Les listes de contrôle d'accès étendues permettent de filtrer sur base des adresses IP sources, des ports sources, des adresses IP de destination, des ports de destination, ainsi que sur différents protocoles et services.

Les stratégies de sécurité sont les suivantes :

1. Autoriser le trafic Web en provenance du réseau 192.168.10.0/24 à accéder à n'importe quel réseau.
2. Autoriser une connexion SSH à l'interface série de R3 à partir de PC-A.
3. Autoriser les utilisateurs du réseau 192.168.10.0.24 à accéder au réseau 192.168.20.0/24.
4. Autoriser le trafic Web en provenance du réseau 192.168.30.0/24 à accéder à R1 via l'interface Web et le réseau 209.165.200.224/27 sur le routeur ISP. Le réseau 192.168.30.0/24 ne devrait PAS être autorisé à accéder à un autre réseau via le Web.

Sur base des stratégies de sécurité mentionnées ci-dessus, vous aurez besoin au minimum de deux listes de contrôle d'accès pour satisfaire aux stratégies de sécurité. Il est conseillé de placer les listes de contrôle d'accès étendues le plus près possible de la source. Nous suivre cette pratique dans le cadre de ces stratégies.

Étape 1: Configurez une liste de contrôle d'accès étendue numérotée sur R1 pour les numéros de stratégie de sécurité 1 et 2.

Vous utiliserez une liste de contrôle d'accès étendue numérotée sur R1. Quelles sont les plages pour les listes de contrôle d'accès étendues ?

a. Configurez la liste de contrôle d'accès sur R1. Utilisez 100 comme numéro de liste de contrôle d'accès.

```
R1(config)# access-list 100 remark Allow Web & SSH Access
R1(config)# access-list 100 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22
R1(config)# access-list 100 permit tcp any any eq 80
```

Que signifie 80 dans le résultat de commande indiqué ci-dessus ?

À quelle interface la liste de contrôle d'accès ACL 100 doit-elle être appliquée ?

Dans quelle direction la liste de contrôle d'accès ACL 100 doit-elle être appliquée ?

b. Appliquez la liste de contrôle d'accès ACL 100 à l'interface S0/0/0.

```
R1(config)# int s0/0/0
R1(config-if)# ip access-group 100 out
```

c. Vérifiez la liste de contrôle d'accès ACL 100.

1) Ouvrez un navigateur Web sur PC-A, puis accédez à http://209.165.200.225 (le routeur ISP). La requête doit aboutir ; dépannez si ce n'est pas le cas.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

2) Établissez une connexion SSH entre PC-A et R3 en utilisant 10.2.2.1 comme adresse IP. Connectez-vous au moyen des informations d'identification **admin** et **class**. La requête doit aboutir ; dépannez si ce n'est pas le cas.

3) À partir de l'invite du mode d'exécution privilégié sur R1, exécutez la commande **show access-lists**.

```
R1# show access-lists
Extended IP access list 100
    10 permit tcp host 192.168.10.3 host 10.2.2.1 eq 22 (22 matches)
    20 permit tcp any any eq www (111 matches)
```

4) À partir de l'invite de commande de PC-A, envoyez une requête ping à 10.2.2.1. Pouvez-vous expliquer vos résultats ?

Étape 2: Configurez une liste de contrôle d'accès étendue nommée sur R3 pour la stratégie de sécurité numéro 3.

a. Configurez la stratégie sur R3. Attribuez à la liste de contrôle d'accès le nom WEB-POLICY.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 host 10.1.1.1 eq 80
R3(config-ext-nacl)# permit tcp 192.168.30.0 0.0.0.255 209.165.200.224
0.0.0.31 eq 80
```

b. Appliquez-la à l'interface S0/0/1.

```
R3(config-ext-nacl)# int S0/0/1
R3(config-if)# ip access-group WEB-POLICY out
```

c. Vérifiez-la.

1) À partir de l'invite de commande du mode d'exécution privilégié du routeur R3, exécutez la commande **show ip interface s0/0/1**.

Quel est, le cas échéant, le nom de la liste de contrôle d'accès ?

Dans quelle direction, la liste de contrôle d'accès est-elle appliquée ?

2) Ouvrez un navigateur Web sur PC-C, puis accédez à http://209.165.200.225 (le routeur ISP). La requête doit aboutir ; dépannez si ce n'est pas le cas.

3) À partir de PC-C, ouvrez une session Web sur http://10.1.1.1 (R1). La requête doit aboutir ; dépannez si ce n'est pas le cas.

4) À partir de PC-C, ouvrez une session Web sur http://209.165.201.1 (routeur ISP). Elle devrait échouer ; dépannez si ce n'est pas le cas.

5) À partir de l'invite de commande de PC-C, envoyez une requête ping à PC-A. Quel résultat obtenez-vous et pourquoi ?

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Partie 4: Modification et vérification des listes de contrôle d'accès étendues

En raison des listes de contrôle d'accès appliquées sur R1 et R3, aucune requête ping ou aucun autre type de trafic n'est autorisé entre les réseaux locaux sur R1 et R3. La direction a décidé d'autoriser tout le trafic entre les réseaux 192.168.10.0/24 et 192.168.30.0/24. Vous devez modifier les deux listes de contrôle d'accès sur R1 et R3.

Étape 1: Modifiez la liste de contrôle d'accès ACL 100 sur R1.

a. À partir du mode d'exécution privilégié sur R1, exécutez la commande **show access-lists**.

Combien y a-t-il de lignes dans cette liste d'accès ?

b. Passez en mode de configuration globale et modifiez la liste de contrôle d'accès sur R1.

```
R1(config)# ip access-list extended 100
R1(config-ext-nacl)# 30 permit ip 192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
R1(config-ext-nacl)# end
```

c. Exécutez la commande **show access-lists**.

Où apparaît la nouvelle ligne que vous venez d'ajouter dans la liste de contrôle d'accès ACL 100 ?

Étape 2: Modifiez WEB-POLICY sur R3.

a. À partir du mode d'exécution privilégié sur R3, exécutez la commande **show access-lists**.

Combien y a-t-il de lignes dans cette liste d'accès ?

b. Passez en mode de configuration globale et modifiez la liste de contrôle d'accès sur R3.

```
R3(config)# ip access-list extended WEB-POLICY
R3(config-ext-nacl)# 30 permit ip 192.168.30.0 0.0.0.255 192.168.10.0
0.0.0.255
R3(config-ext-nacl)# end
```

c. Exécutez la commande **show access-lists** pour vérifier que la nouvelle ligne a été ajoutée à la fin de la liste de contrôle d'accès.

Étape 3: Vérifiez les listes de contrôle d'accès modifiées.

a. À partir de PC-A, envoyez une requête ping à l'adresse IP de PC-C. Les requêtes ping ont-elles abouti ?

b. À partir de PC-C, envoyez une requête ping à l'adresse IP de PC-C. Les requêtes ping ont-elles abouti ?

Pourquoi les listes de contrôle d'accès ont-elles fonctionné immédiatement pour les requêtes ping dès que vous les avez modifiées ?

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.

Remarques générales

1. Pourquoi une planification et des tests attentifs des listes de contrôle d'accès sont-ils requis ?

2. Quel type de liste de contrôle d'accès est optimal : standard ou étendue ?

3. Pourquoi les paquets hello EIGRP et les mises à jour de routage ne sont-ils pas bloqués par l'entrée de contrôle d'accès (ACE) **deny any** implicite ou l'instruction ACL des listes de contrôle d'accès appliquées à R1 et R3 ?

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.

© 2014 Cisco et/ou ses filiales. Tous droits réservés. Ceci est un document public de Cisco.