TP : Les listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès, ou ACL (Access Control List), pour IP permettent à un routeur de supprimer certains paquets en fonction de critères définis à l'avance. Le but de ces listes, appelées filtres, est de protéger le réseau contre tout trafic indésirable. Elles peuvent servir à différents usages :

- Filtrer le trafic réseau en fonction des adresses et des protocoles de couches supérieures (autoriser le trafic de messagerie, bloquer le trafic telnet …) ;
- Contrôler le flux du trafic en empêchant les informations de mises à jour de routage d'un réseau particulier de se propager n'importe ou;
- Fournir un niveau de sécurité d'accès réseau de base.

Une liste d'accès implique un traitement en deux étapes : recherche de correspondance et action. La première consiste à examiner chaque paquet afin de déterminer s'il correspond à l'une des instructions **access-list** de la liste. Si une correspondance est trouvée, deux actions sont possibles : autoriser le paquer (***permit***) ou l'interdire (***deny***).

Les critères de comparaison spécifiés dans les ACL peuvent se fonder sur des champs d'entêtes IP, TCP et UDP. Il existe deux catégories principales de listes de contrôle d'accès pour IP : *standard* et *étendus*. Les *ACL étendus* peuvent examiner les adresses IP sources et destination ainsi que les numéros de ports sources et destinataires, et plusieurs autres champs. Les *ACL standard* ne peuvent examiner que l'adresse IP source.

Pour spécifier quelle partie d'une adresse IP examiner, Cisco prévoit l'emploi de ***masques génériques***. Un tel masque est associé à une adresse IP dans les instructions de la liste d'accès (voir annexe). Un masque générique ressemble à un masque de sous-réseau mais n'a pas la même fonctionnalité. Dans un masque générique, les bits à 0 indiquent au routeur qu'il doit comparer les bits situés aux positions correspondantes dans l'adresse d'un paquet. Les bits à 1 lui indiquent que les bits correspondants sont à ignorer.

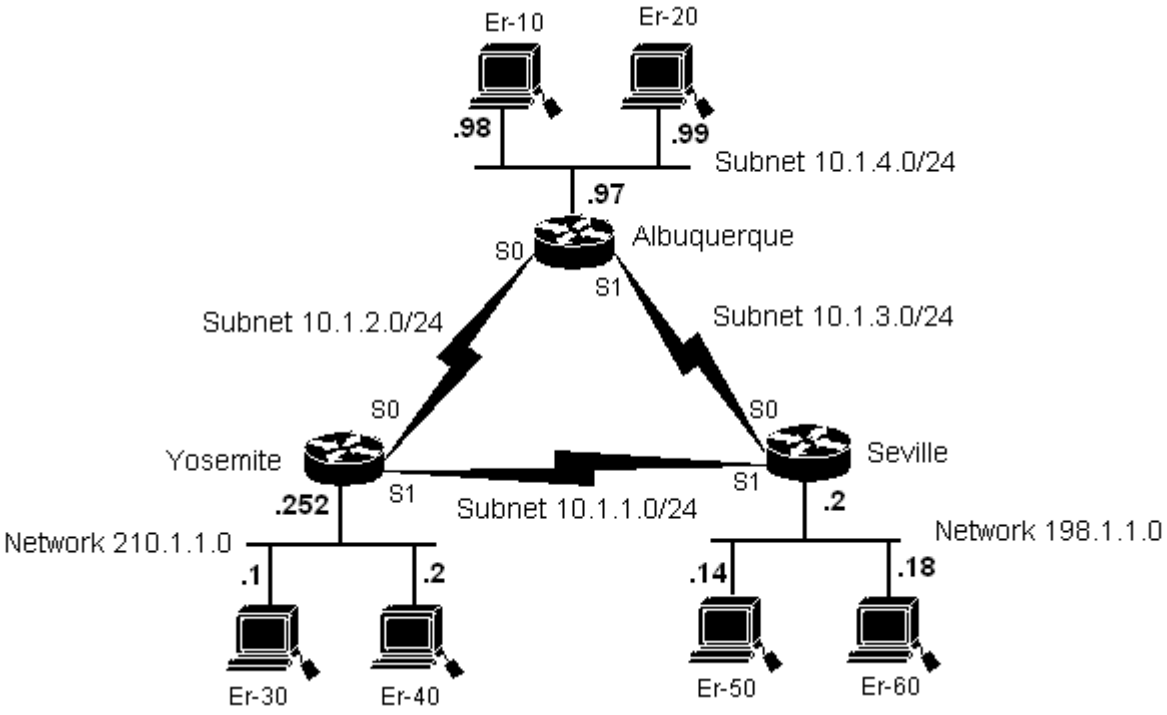
Quand le routeur applique une ACL sur un trafic, il associe l'ACL à *une interface*, spécifiquement pour *le trafic entrant ou sortant*.

Travail à réaliser

Considérant les scénarios 1, 2 et 3 à mettre en œuvre sur la figure donnée ci-dessous, avec pour chaque scénario des règles de restrictions d'accès. Dans chaque cas, configurez les listes d'accès appropriés permettant de répondre aux exigences spécifiées dans chacun des scénarios. Placez les listes d'accès dans le routeur qui filtre les paquets à rejeter aussi rapidement que possible.

Scénario 1 - Les critères de filtrage sont **:**

1. ER-30 doit pouvoir accéder aux machines du sous-réseau de Séville.
2. Toutes les autres machines du sous-réseau de Yosemite ne sont pas autorisées à accéder au sous-réseau de Séville.
3. Tous les autres accès sont autorisés.



Scénario 2 - Les critères de filtrage sont **:**

1. Les machines du sous-réseau de Albuquerque ne sont pas autorisées à communiquer avec les machines du sous-réseau de Yosemite.
2. Les machines ER-30 et ER-40 ne sont pas autorisées à accéder aux machines du sous-réseau de Séville.
3. Les autres accès entre les machines des sous-réseaux de Séville et Yosemite sont autorisés.
4. Tous les autres accès sont autorisés.

Scénario 3 - Les critères de filtrage sont **:**

1. Les machines ER-30 et ER-40 ont le droit de se connecter à tout serveur Web du sous-réseau de Séville.
2. Les machines ER-30 et ER-40 ne sont pas autorisées à se connecter à d'autres serveurs du sous-réseau de Séville avec TCP.
3. ER-10 peut accéder uniquement aux services Web (et pas aux autres services) du sous-réseau de Séville.
4. Les machines du sous-réseau de Yosemite peuvent accéder aux machines du sous-réseau de Séville sauf indication contraire.
5. Les clients Web sur le sous-réseau d'Albuquerque ne sont pas autorisés à se connecter au serveur Web sur le sous-réseau de Séville à moins que ce soit mentionné ailleurs dans ces critères.
6. Toute autre communication non spécifiée devrait être interdite.

Annexe : Définition et utilisation des listes de contrôle d'accès

A. Les ACL standards :

La liste d'accès standard permet d'accepter ou de refuser tout le trafic d'un réseau particulier. Toutefois, elle ne permet de comparer que l'adresse IP source à un agencement de bits particulier (appelé ***masque générique***).

1) Configuration des ACL :

- **Définition de la liste** :

Router (config.)# **access-list** "*numéro-liste-accès entre 1 et 99*" {**permit**|**deny**} *"@ IP source/masque générique*"

Router (config.)# **access-list** "*numéro-liste-accès entre 1 et 99*" **remark** *"texte*"

Définit un commentaire qui rappelle l'effet de la liste d'accès.

Une fois la liste de contrôle d'accès crée, il faut l'assigner à une interface (pour l'activer) de la manière suivante :

- **Assignation de la liste à une interface :**

Router (config-if)# **ip access-group** <n°-liste> [**in**|**out**]

- **in** | **out** indique si la liste doit être appliquée pour le trafic entrant ou sortant.

- **Afficher le contenu de la liste d'accès :**

La commande **show access-lists** affiche le contenu de toutes les listes d'accès. Pour consulter une liste particulière il faut spécifier son numéro de liste (<n°-liste>).

- **Les bits de masque générique :**

Les listes de contrôle d'accès utilisent le masque générique pour spécifier quelle partie d'une adresse IP examiner (dans le but d'accorder ou d'interdire l'accès) comme suit :

- Masque de 32 bits divisé en 4 octets
  - 0 signifie **« vérifier la valeur du bit correspondant »**
  - 1 signifie **« ignorer la valeur du bit correspondant »**

- Exemple : Router (config.)# **access-list** 1 **permit** 5.6.0.0 0.0.255.255 ;
  Seul les 16 premiers bits sont vérifiés

- **La commande « any » :**

Cette commande est utilisé pour indiquer n'importe quelle adresses (équivaut à **0.0.0.0 255.255.255.255**) :

- Exemple : Router (config.)# **access-list** 1 **permit** 0.0.0 0 255.255.255.255 ;
  Équivaut à :
- Router (config.)# **access-list** 1 **permit any** ;

- **La commande « host » :**

Cette commande permet d'indiquer une adresse bien spécifique :

- Exemple : Router (config.)# **access-list** 1 **permit** 172.30.16.29 0.0.0 0 ;
  Équivaut à :
- Router (config.)# **access-list** 1 **permit host** 172.30.16.29 ;

B. Les ACL étendues :

Les listes d'accès étendues permettent de filtrer les paquets au niveau de la couche transport du modèle OSI (vérifient les protocoles et les n° de ports source et destination), tout en précisant l'adresse IP de destination, ainsi que d'autres paramètres.

1) Configuration des ACL :

La procédure est la même que la liste d'accès standard, avec la syntaxe suivante :

- **Syntaxe :**

Router (config.)# **access-list** "*numéro liste accès*" {**permit**|**deny**} "*protocole sur IP*" *"@ IP source/masque générique*" ["*opérateur*" ["*port*"]] *"@ IP destination/masque générique*" ["*opérateur*" ["*port*"]] [**established**] [**log**]

Paramètre	Description
N° de liste	**De 100 à 199**
protocole sur IP	**Identifie le protocole concerné : IP, TCP, ICMP, UDP,IGRP,OSPF,EIGRP**
opérateur	**Fonction conditionnelle : eq, lt, gt, ne, range**
port	**N° de port (peut être remplacé par son nom)**
Established	**Permet au trafic TCP de passer si le paquet utilise une connexion établie**
log	**Permet de préciser si les correspondances trouvées pour la liste d'accès doivent être consignées**

Remarque : Seuls les protocoles qui utilisent directement IP sont pris en compte. Par exemple, RIP n'apparaît pas car il utilise UDP.

- **Exemple :**

Router (config.)# **access-list** 101 deny **tcp** **any** **host** **172.16.4.1** **range** 20 23
access-list 101 permit **tcp** **any** **host** **172.16.4.1** **eq** smtp

Ainsi, on bloque les services TCP (20 à 23) à destination de 172.16.4.1, et on autorise uniquement le service de messagerie (SMTP) vers cette même machine.

2) IP Accounting :

IP accounting est un outil (debugging) permettant de vérifier si une ACL étendue est correcte. Il permet de garder trace des adresses sources et destinations des correspondances trouvées pour la liste d'accès mais aussi celles qui violent la même liste.

IP accounting permet ainsi de vérifier quels paquets sont autorisés et ceux qui sont bloqués.

- **Syntaxe :** (mode configuration interface):
  Router (config-if)# **ip accounting output-packets**
  Router (config-if)# **ip accounting access-violations**

- **Afficher le contenu de la trace :**
  Router # show ip **accounting**
  Router # show ip **accounting access-violations**

3) **Loggings :**

Il s'agit d'une autre technique (mot clé **log**) pour vérifier si une ACL étendue est correcte. Elle permet de préciser si les correspondances trouvées pour la liste d'accès doivent être consignées dans le buffer du router.

L'accès aux logs du routeur se fait par la commande **show logging.**

- **Exemple:**
  Router (config)# **access-list** 101 **deny tcp any host** 172.16.4.1 **range** 20 23 **log**

C. Contrôle des mises à jour de routage grâce aux ACL :

Les listes d'accès peuvent aussi servir à filtrer les informations de routage. Pour réaliser ce filtrage, on procède de la manière suivante :

1. Créer la liste d'accès en standard ou étendue comme décrit auparavant.

2. En mode configuration routeur, appliquer la liste définie, par la commande **distribute-list** <n°-liste> [**in**|**out**] <interface>, à l'interface donnée en argument. Les mots clefs in (entrée) et out (sortie) permettent de déterminer le sens du filtre.