IUT de Lannion – BUT Informatique

2ème année – Réseaux avancés - sécurité

TP - ACL

Objectif

L'objectif de ce TP est d'étudier les ACL Cisco qui permettent de faire du filtrage.

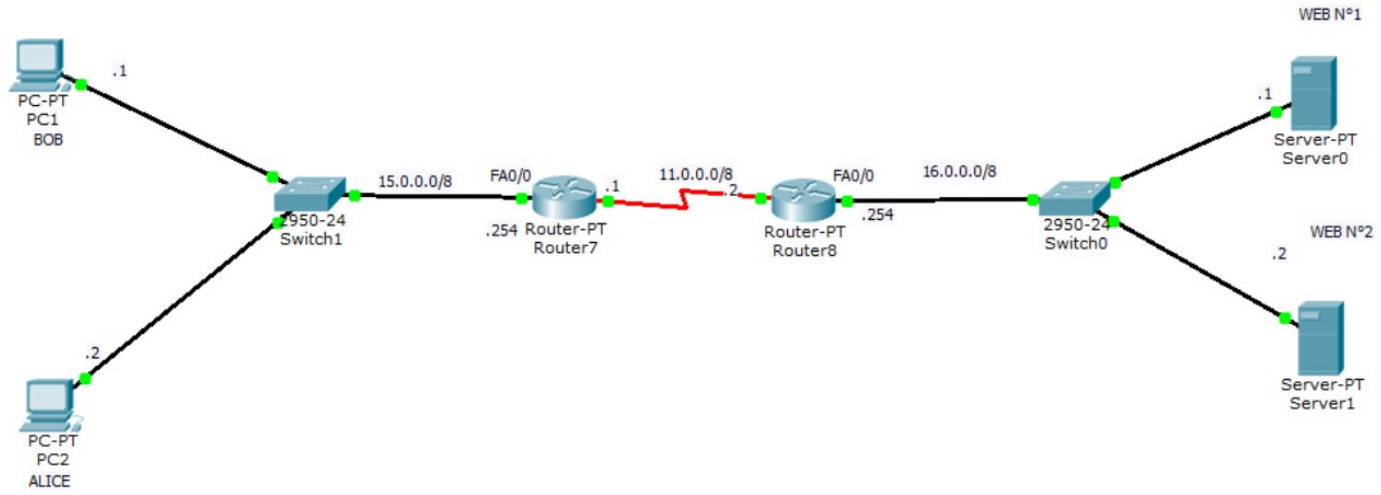
Dans ce TP, vous aborderez les configurations suivantes (avec Cisco Packet Tracer):

- Etape 1 : Mise en place d'une infrastructure réseau.
- Etape 2 : Configuration d'un filtrage au niveau du routeur d'accès de votre entreprise : filtrage avec des ACL simple et filtrage avec des ACL étendues.

A la fin du TP, vous allez déposer votre travail dans l'espace de dépôt dédié :

- Sauvegardez donc votre travail dans deux fichiers de simulations nommés : acl-tp1-exercice1.pkt et acl-tp1-exercice2.pkt. A la fin de la séance, vous déposerez votre travail : fichier nommé NOM.zip. L'archive déposée contiendra votre compte rendu (un fichier nommé NOM.pdf) ainsi que les fichiers de simulation. Le travail rendu doit être une version originale de votre réalisation et non pas inspiré d'une autre réalisation.

I. MISE PLACE DU RESEAU



- La plateforme considérée est représentée dans schéma ci-dessus. Elle comprend :
  - 2 routeurs génériques connectés, par exemple, par une liaison série.
  - 2 PCs connectés au commutateur du site de gauche. Ce commutateur est également connecté au routeur du site de gauche.
  - 2 serveurs connectés au commutateur du site de droite. Ce commutateur est également connecté au routeur du site de droite.
- Configurez votre plateforme conformément au schéma ci-dessus :
  - Configurez les PCs (adresse IP et passerelle).
  - Configurez les serveurs (adresse IP et passerelle).
  - Configurer le réseau entre les routeurs.

- Configurer les 2 routeurs avec pour chacun, une route par défaut vers l'autre routeur.
- Donnez un extrait pertinent du résultat du sh run sur les trois routeurs.
- Donnez la table de routage des deux routeurs.
- Testez la connectivité sur chacun des liens. Testez la connectivité de bout en bout : entre les machines (PC1 et PC2) et les serveurs (Server0 et Server1).
- Donnez le résultat d'un ping entre le PC1 et le Server1.

II. EXERCICE 1 - MISE EN PLACE D'UN FILTRAGE AVEC LES ACL SIMPLES

Dans cet exercice, vous allez configurer une ACL simple (filtrage basé sur l'adresse ip source) interdisant au PC de Bob d'atteindre le réseau externe. Bob ne pourra dialoguer qu'avec Alice. Par contre Alice pourra atteindre le réseau externe.

- Créer une ACL simple nommée ACL#1 sur le routeur du site de gauche (coté PCs) avec la commande suivante :

```
Router(config)# ip access-list standard ACL#1
```

- Configurer une « description » de votre ACL. Par exemple, « ACL pour interdire à Bob de sortir de son réseau ». Pour trouver comment faire, tapez « ? » après la commande suivante :

```
Router(config)# ip access-list standard ACL#1
```

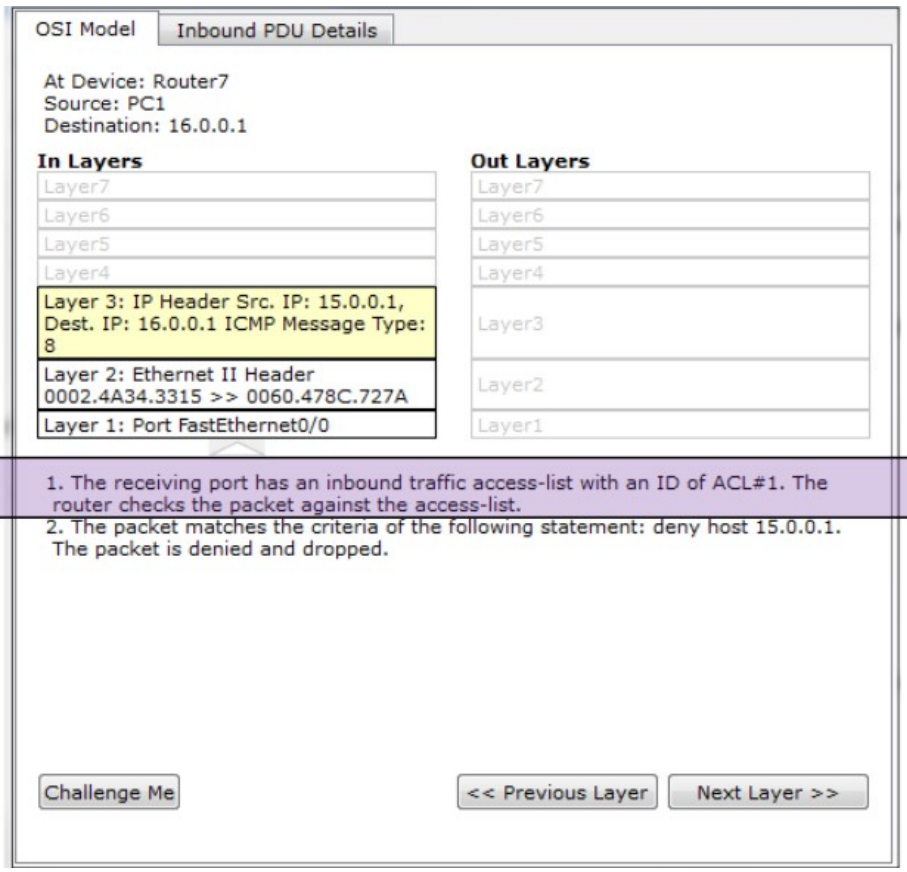
  - Parmi les commandes proposées, quelle est celle permettant de configurer une « description » pour cette ACL ?
  - Tapez cette commande et la description suggérée

- Vous allez maintenant configurer les règles de cette ACL. Vous allez donc ajouter une règle pour interdire au PC1 de communiquer avec l'extérieur de son réseau. Pour ce faire, vous devez d'abord répondre aux questions suivantes :
  - Quelle action vous devez choisir entre : permit, deny et remark ?
  - Donnez la syntaxe qui vous permet de désigner l'adresse de la machine de Bob (vous avez deux possibilités) ?
- Donnez la commande permettant d'interdire au PC de Bob de communiquer avec l'extérieur. Configurez votre routeur avec cette commande.
- Associez votre ACL à l'une des interfaces de votre routeur. Pour ce faire, vous devez d'abord répondre à la question suivante :
  - Sur quelle interface est-il le plus judicieux d'appliquer votre ACL ? Justifiez votre réponse.
  - Appliquez maintenant votre ACL sur l'interface située du côté des PCs et dans le sens convenable en utilisant les commandes suivantes :

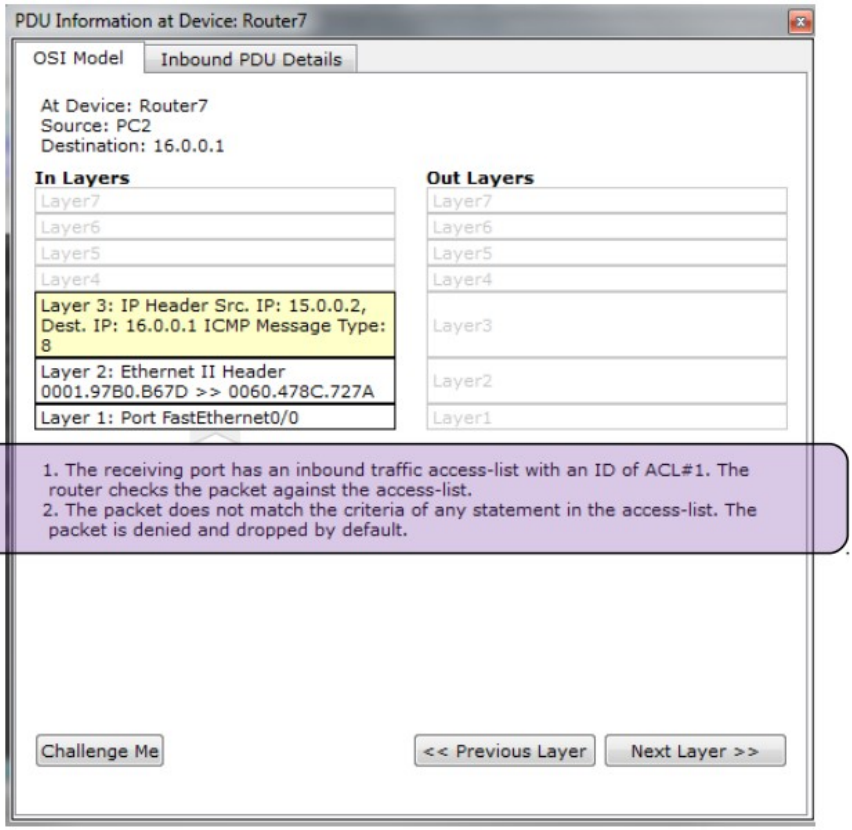
```
Router(config)# interface <nom de l'interface>
```

```
Router(config-if)#ip access-group ACL#1 <sens> (sens à choisir entre in et out)
```

- Vérifiez la configuration de votre routeur. Donnez la commande qui vous a permis de le faire et le résultat de cette commande.
- Depuis le PC de Bob, faites les tests suivants :
  - Ping 15.0.0.2. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?
  - Ping 16.0.0.1. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?
- Passez en mode simulation et vérifiez que vous obtenez le message suivant au niveau de votre routeur :



- Depuis le PC d'Alice, faites les tests suivants :
  - Ping 15.0.0.1. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?
  - Ping 16.0.0.1. Quel est le résultat ? Pourquoi vous obtenez ce résultat ?
- Passez en mode simulation et vérifiez que vous obtenez le message suivant au niveau de votre routeur :



- Vous pourrez donc conclure que tout ce qui n'est pas autorisé est interdit. Vous devez donc ajouter une règle supplémentaire à votre ACL (ACL#1). Choisissez la règle à ajouter parmi les règles ci-dessous (4 des 5 règles répondent à la demande).

```
Router(config)#ip access-list standard ACL#1
Router(config-std-nacl)#permit any
```

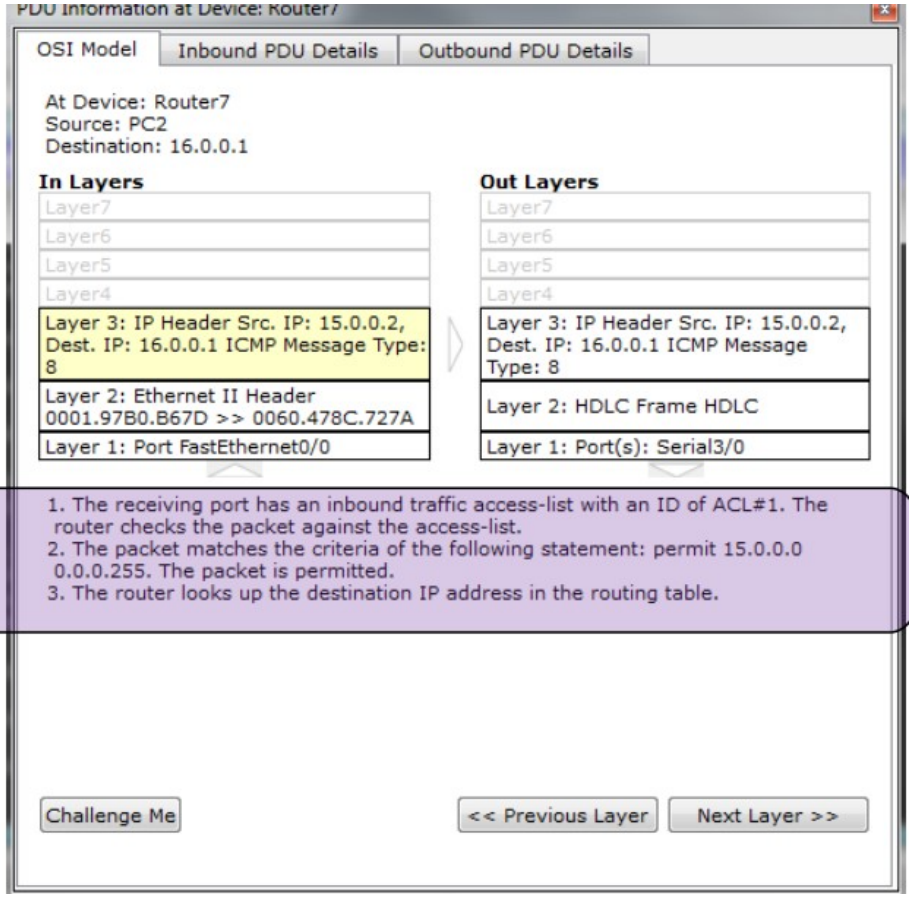
```
Router(config)#ip access-list standard ACL#1
Router(config-std-nacl)#permit 15.0.0.2 0.0.0.0
```

```
Router(config)#ip access-list standard ACL#1
Router(config-std-nacl)#permit 0.0.0.0 255.255.255.255
```

```
Router(config)#ip access-list standard ACL#1
Router(config-std-nacl)#deny 0.0.0.0 255.255.255.255
```

```
Router(config)#ip access-list standard ACL#1
Router(config-std-nacl)#permit 15.0.0.0 0.0.0.255
```

- La dernière règle est l'une de celles permettant de répondre à votre cahier de charges. Pourquoi cette règle répond à vos besoins ? Que se passe-t-il si cette règle était positionnée avant la première règle (celle créée pour interdire à Bob d'accéder à l'extérieur de son réseau) ?
- En mode simulation, vérifiez que vous obtenez bien le message suivant au niveau du router coté PCs :



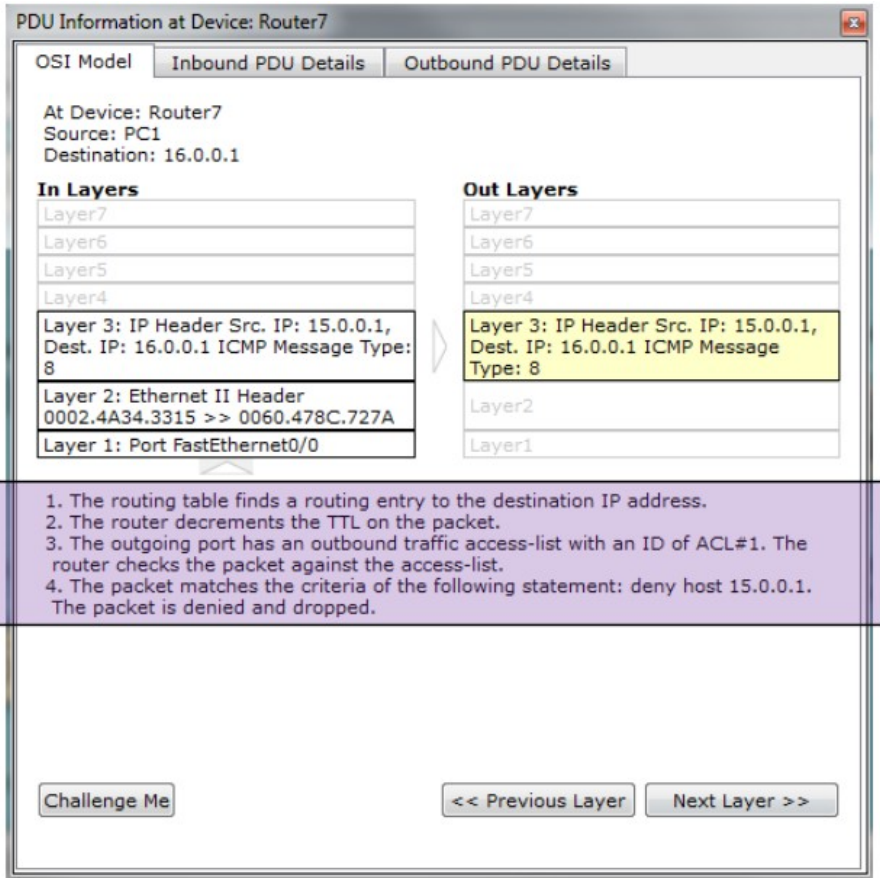
- La commande suivante permet aussi de visualiser les ACLs :

```
Router#sh access-lists ACL#1
```

- Donnez le résultat de cette commande sur votre routeur et expliquez à quoi correspondent les « matches ».
- Configurez votre ACL sur l'interface de sortie avec les commandes suivantes :

```
Router(config-if)#no ip access-group ACL#1 sens
Router(config-if)#exit
Router(config)#interface <nom de l'interface située du coté extérieur
Router(config-if)#ip access-group ACL#1 out
```

- Faites les tests nécessaires pour prouver le bon fonctionnement de cette nouvelle solution de filtrage.
- Expliquez les différences entre cette solution de filtrage et la solution configurée précédemment. Voici un indice concernant l'une des différences :



III. EXERCICE 2 - MISE EN PLACE D'UN FILTRAGE AVEC LES ACL ETENDUES

- Pour commencer, supprimez le filtrage de l'exercice précédent avec la commande suivante :

```
Router(config-if)#no ip access-group ACL#1 sens
```

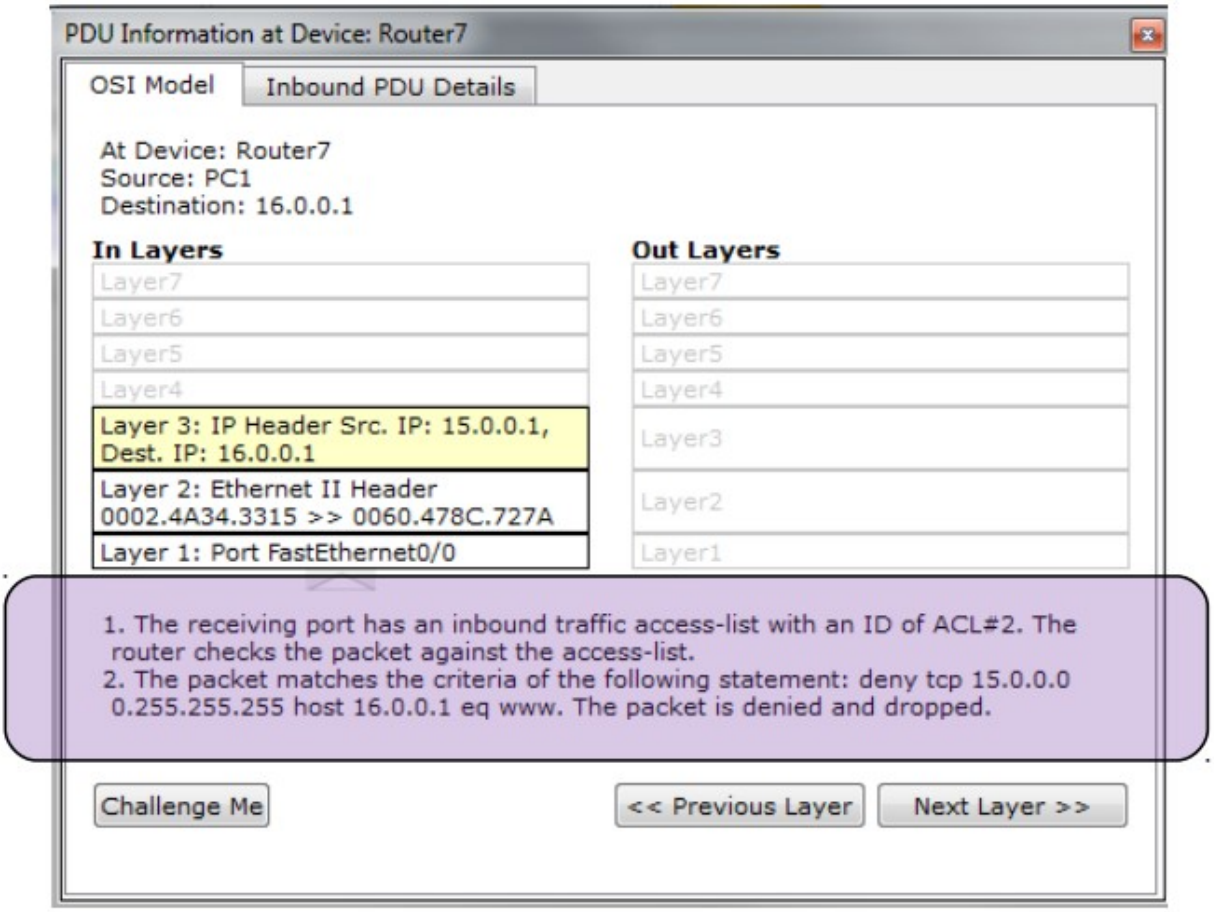
- Ajoutez une ACL étendue nommée ACL#2 sur votre routeur. Cette ACL sera composée de plusieurs règles et positionnée du côté des PCs.

```
Router(config)#ip access-list extended ACL#2
```

- Ajoutez à votre ACL une règle pour interdire à tous les PCs du réseau 15.0.0.0/8 d'accéder au service web du Server1. Vous devez spécifier tous les paramètres permettant d'identifier le protocole, les adresses IP sources et destination et les ports sources et destination. Donnez la règle que vous avez ajoutée en expliquant tous ses paramètres.
- Appliquez l'ACL#2 sur l'interface située du côté des PCs en utilisant la commande suivante :

```
Router(config-if)#ip accessgroup ACL#2 in
```

- Passez en mode simulation. Appliquez un filtre pour ne visualiser que les paquets TCP.
- Utilisez le client http des PC pour solliciter l'URL 16.0.0.1. Vous devriez obtenir le message suivant au niveau de votre routeur :



- Que se passe-t-il lorsque vos PCs sollicitent l'URL 16.0.0.2 ?
- Ajoutez donc une règle pour autoriser l'accès aux autres serveurs. Donnez la règle ajoutée et prouvez le bon fonctionnement de votre solution de filtrage.
- Que se passe-t-il si vous « pinguez » les serveurs depuis les PCs ?