DNS - HTTP - ACL
Mise en œuvre sur Packet Tracer

L'objectif de ce TD est de mettre en place un service web dans un réseau d'entreprise et de sécuriser les flux circulant dans ce réseau en utilisant les ACL. La section 1 vous fournit les éléments de base sur les ACL.

1 Rappel sur les ACL

Les ACL (Acces-List- Control) sont des listes de classification de flux. La classification de flux est utilisé par un plusieurs services réseau tels que la translation d'adresses, les VPN, la Qualité de Service, le filtrage, le routage. Elle est en général configurée sur un routeur mais certains commutateurs disposent de cette fonctionnalité.
Il existe 2 types d'ACL : les *ACL standards* et les *ACL étendues*.
Lorsque des ACL sont définies sur un routeur, chaque paquet est analysé et comparé aux ACL dans l'ordre séquentiel. Dès qu'un paquet correspond à une des ACL, l'action est réalisée.

Attention, dès qu'une ACL est définie, une ACL implicite (il n'est pas nécessaire de l'écrire ; elle existe de façon automatique) est prise en compte. Cette dernière interdit tout flux.

1.1 ACL standards

Les ACL standards permettent de bloquer ou d'autoriser tout ou partie du flux réseau en fonction de l'adresse IP source. La syntaxe est la suivante :

```
Router(config)#access-list numéro permit/deny @ip_source masque
```

Une ACL étendue a un numéro entre 1 et 99. Seule l'adresse IP source est spécifiée. Le masque est un masque inversé (wilcard).
Exemple : L'ACL suivant autorise le flux issu du réseau 192.168.0.0/24

```
Router(config)#access-list 1 permit 192.168.0.0 0.0.0.255
```

1.2 ACL étendues

Les ACL étendues sont plus spécifiques que les ACL standards. Elles permettent de classifier les flux en fonction des adresses IP source, des adresses IP destination, du protocole de la couche 3 ou 4 (IP, TCP, UDP, ICMP), des ports sources, des ports destination.
Une ACL étendue a un numéro entre 100 et 199. Les différentes opérandes possibles pour les ports sont :

- *eq* : =
- *lt* : <
- *gt* : >

La syntaxe générale est la suivante :

```
Router(config)#access-list numéro permit/deny ip/tcp/udp @ip_source masque
              [eq/lt/gt] [port_source] @ip_destination masque [eq/lt/gt]
              [port_destination] [log]
```

Dans l'exemple suivant, la liste de contrôle d'accès classifie le flux tcp pour des ports sources supérieurs à 1024 provenant du réseau 192.168.0.0/24 et à destination du serveur HTTP (port tcp/80) situé à l'adresse 10.0.0.1.

```
Router(config)#access-list 100 permit tcp 192.168.0.0 0.0.0.255
               gt 1024 10.0.0.1 0.0.0.0 eq 80
```

1.3 ACL pour le NAT

Pour mettre en place la translation d'adresse, il faut spécifier quels sont les réseaux qui doivent être translatés en classifiant le flux par une liste de contrôle d'accès.
Les étapes de mise en place du NAT sur un routeur CISCO sont les suivantes :

L'interface routeur du réseau qui est translatée doit avoir la configuration suivante :

```
Router(config-subif)#ip nat inside
```

L'interface de sortie doit avoir la configuration suivante :

```
Router(config-if)#ip nat outside
```

Il faut ensuite définir une ACL qui spécifie le flux réseau devant être translaté. L'exemple suivant classifie le réseau 192.168.0.0/24 pour un accès complet (protocole *ip*, destination *any*)

```
Router(config)#access-list 150 permit ip 192.168.0.0 0.0.0.255 any
```

La dernière étape est l'activation du NAT sur le routeur.
L'exemple suivant active le protocole NAT qui translate les réseaux définis par l'acl 150 sur l'adresse publique de l'interface f0/1

```
Router(config)#ip nat inside source list 150 f0/1 overload
```

1.4 ACL pour le filtrage

Lorsque les ACL sont utilisées pour du filtrage de flux (autoriser ou bloquer à transiter au travers d'une interface réseau d'un routeur), deux étapes sont nécessaires :

1. La définition des flux devant être analysés (voir sections 1.1 et 1.2) ;
2. L'application de l'ACL sur l'une des interfaces du routeur.

Pour le filtrage, les paquets sont analysés au moment de leur transit au travers d'un interface du routeur, en fonction de leur sens de circulation (flux entrant (`IN`) ou flux sortant (`OUT`)).
La syntaxe pour appliquer une ACL sur une interface est la suivantes :

```
Router(config-if)#ip access-group numero_ACL IN|OUT
```

Lorsque l'ACL est une ACL standard, l'ACL sera appliquée au plus proche de la destination. Lorsque l'ACL est une ACL étendues, l'ACL sera appliquée au plus proche de la source.

Dans l'exemple suivant, on souhaite laisse passer les flux correspondant aux requêtes http du réseau 192.168.0.0/24 vers le réseau 192.168.1.0/24. La passerelle du réseau 192.168.0.0/24 correspond à l'interface f0/0.2 du routeur.
Etape 1 : définition de l'ACL

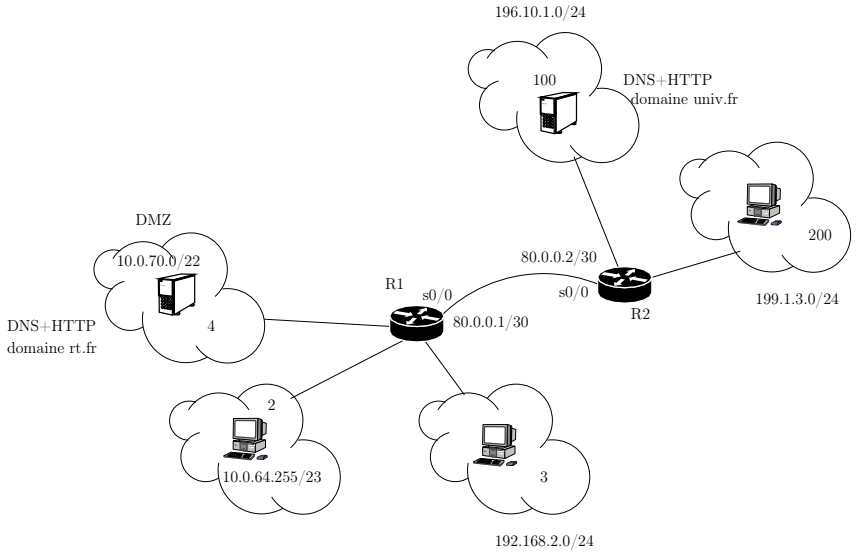
```
Router(config)#access-list 150 permit tcp 192.168.0.0 0.0.0.255 gt 104
192.168.1.0 0.0.0.255 eq 80
```

Etape 2 : application de l'ACL

```
Router(config)#int f0/0.2
Router(config-)#ip access-group 150 IN
```

2 Exercice

On considère le réseau de la figure suivante :



Dans notre configuration, l'adresse d'interface d'un routeur est choisie comme la dernière adresse valide du réseau auquel l'interface est connectée.
Les adresses de réseau des VLAN 3, 100 et 200 vous sont fournies.
Un serveur d'adresse 10.0.70.0/22, comportant un service DNS et HTTP est situé dans le VLAN 4.
Un poste client d'adresse 10.0.64.255/23 est situé dans le VLAN 2.
Le routeur R2 est configuré.

2.1 Configuration de base des routeurs et des commutateurs

1. En utilisant les informations sur les adresses IP des postes et sur les adresses de réseau des VLAN, déduire les adresses IP des passerelles de l'ensemble des VLANS.
2. Configurez le commutateur S1 avec les spécifications suivantes (le routeur R1 est connecté au 1er port gigabit de S1) :

vlan id	*name*	*port*
2	vlan2	1-5
3	vlan3	6-10
4	dmz	11-13

3. Configurez le commutateur S2 avec les spécifications suivantes (le routeur R2 est connecté au 1er port gigabit de S2) :

vlan id	*name*	*port*
100	vlan100	1-3
200	vlan200	4-6

4. Configurez les adresses des interfaces du router R1
5. Mettez en place une translation d'adresse pour les machines du vlan2, vlan 3 et de la dmz. L'adresse destination du NAT est l'adresse de l'interface s0/0 de R1.

2.2 Configuration des services

6. Configurez le service DNS du serveur situé dans le vlan4 à l'adresse 10.0.70.0/22. Le nom de domaine est *rt.fr*. Le nom du serveur est *dns.rt.fr*
7. Configurez le service HTTP du serveur situé dans le vlan4 à l'adresse 10.0.70/0/22. La page web sera accessible à l'URL *www.rt.fr*. Configurez en conséquence le DNS
8. Configurez le service DNS du serveur situé dans le vlan100 à l'adresse 196.10.1.1/24 Le nom de domaine est *univ.fr*. Le nom du serveur est *dns.univ.fr*
9. Configurez le service HTTP du serveur situé dans le vlan100 à l'adresse 196.10.1.1/24. La page web sera accessible à l'URL *www.univ.fr*. Configurez en conséquence le DNS
10. Placez une station dans le vlan 2 et une station dans le vlan 3. Indiquez le serveur dns.rt.fr comme serveur DNS pour ces stations. Vérifiez que vous avez bien accès à partir d'un navigateur à la page web *www.rt.fr*
11. Placez une station dans le vlan 200. Indiquez le serveur dns.univ.fr comme serveur DNS pour cette station. Vérifiez que vous avez bien accès à partir d'un navigateur à la page web *www.rt.fr*.
12. Modifiez la configuration du serveur DNS du VLAN DMZ pour que les stations des vlan 2 et 3 aient accès à la page web *www.univ.fr* (sans modifier la configuration réseau de ces stations).
13. Cette solution est-elle la solution qui serait adoptée dans la réalité ? Pourquoi ?

2.3 Configuration des ACL

14. Créez une access-list sur le routeur R2 telle que les flux entrant sur l'interface s0/0 et comportant une adresse IP privée des classes 192.168.0.0/16 et 10.0.0.0/8 en adresse source soient rejetés. A quoi sert cette règle ?
15. Créez les access-list sur le routeur R1 telles que :

    (a) les clients des vlan 2 et 3 n'ont accès qu'au serveur dns de la dmz. Ils ne peuvent pas consulter un autre serveur dns

    (b) Les clients du vlan 2 ont un accès complet sur le port tcp/80

    (c) les clients du vlan 3 peuvent consulter le serveur HTTP de la DMZ

    (d) Seuls des flux dns et http entrants sur l'interface s0/0 à destination du serveur de la dmz sont autorisés

16. Créez les access-list sur le routeur R2 telles que :

    (a) le serveur DNS du vlan100 répond aux requêtes DNS

    (b) le serveur HTTP du vlan100 répond aux requêtes HTTP

    (c) tout autre flux provenant du vlan100 est interdit