1 But

Le but de se TP est de se familiariser avec l'utilisation des listes de contrôle d'accès étendues. Pour illustrer leur utilisation, vous allez simuler la mise en place d'une DMZ (Zone Démilitarisée) pour un réseau d'entreprise qui héberge son propre site web.

2 Les ACL (Access Control List)

2.1 Définition

Une liste d'accès est un ensemble d'instructions basées sur des protocoles de couche 3 et de couches supérieures pour filtrer le trafic.

Ces règles s'appliquent sur les interfaces afin de bloquer le ou une partie du trafic qui les traverse.

Les ACL font partie des fonctionnalités de type "firewall" des IOS Cisco. On se contentera d'étudier les ACL standard et étendue désignées par un numéro ou un nom.

2.2 Types de protocoles

Les types de protocoles que nous allons pouvoir configurer dans les instructions de filtrage sont :

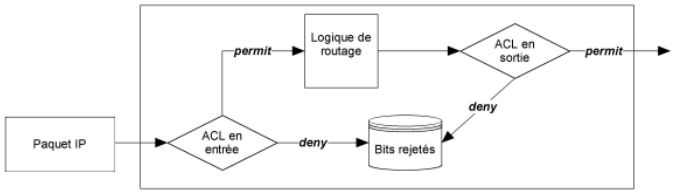
- le port source
- l'adresse IP source
- une partie de l'adresse source
- le port de destination
- l'adresse IP de destination
- une partie de l'adresse de destination

2.3 Utilité

Une liste d'accès va servir :

- A supprimer des paquets pour des raisons de sécurité (pour du trafic de données ou des accès VTY)
- A filtrer des mises à jour de routage
- A filtrer des paquets en fonction de leur priorité (QoS)
- A définir du trafic intéressant pour des configurations spécifiques (NAT, ISDN, etc.)

2.4 Logique d'application



Une liste d'accès, comportant une suite d'instructions de filtrage, va être appliquée sur une interface du routeur, pour le trafic entrant ou pour le trafic sortant. Il va falloir appliquer une logique sur les interfaces en sortie ou en entrée.

2.5 Caractéristiques

- Les paquets peuvent être filtrés en entrée (quand ils entrent sur une interface) avant la décision de routage
- Les paquets peuvent être filtrés en sortie (avant de quitter une interface) après la décision de routage.
- Le mot clef IOS est "deny" pour signifier que les paquets doivent être filtrés ; précisément les paquets seront refusés selon les critères définis.
- Le mot clef IOS est "permit" pour signifier que les paquets ne doivent pas être filtrés ; précisément les paquets seront permis selon les critères définis.
- La logique de filtrage est configurée dans les listes d'accès.
- Une instruction implicite rejette tout le trafic à la fin de chaque liste d'accès

2.6 Traitement

Le traitement d'une liste d'accès se déroule en deux étapes :

1. Recherche de correspondance (examen de chaque paquet)
2. Action (deny ou permit)
3. Si pas de correspondance, instruction suivante
4. Si aucune correspondance, l'instruction implicite est appliquée (Tous les paquets sont rejetés)

2.7 Différence entre liste d'accès standard et liste d'accès étendue

Une liste d'accès standard examinera seulement l'adresse IP source.

- Une liste d'accès étendue pourra examiner les adresses IP et les ports aussi bien source que destination, ainsi que type de protocole (IP, ICMP, TCP, UDP).
- Par ailleurs, il sera possible de vérifier une partie des adresses avec un masque générique (wildcard mask).

2.8 Désignation d'une liste d'accès

On donnera soit un numéro ou un nom à une liste d'accès (un ensemble d'instructions de filtrage) à appliquer sur une interface en entrée ou en sortie.
Si on utilise un numéro on aura le choix dans une plage de nombres en fonction du protocole de couche 3 :

Protocole	*Plage*
IP	1 - 99 et 1300 - 1999
IP étendu	100 - 199 et 2000 - 2699
Apple Talk	600 - 699
IPX	800 - 899
IPX étendu	900 - 999
Protocole IPX Service Advertising	1000 - 1099

Si on utilise un nom, il faudra désigner le type de liste : standard ou étendue.

2.9 Le masque générique (Wildcard Mask)

Un masque générique est un masque de filtrage. Quand un bit aura une valeur de 0 dans le masque, il y aura vérification de ce bit sur l'adresse IP de référence. Lorsque le bit aura une valeur de 1, il n'en y aura pas.

Le masque générique à utiliser est généralement l'inverse du masque de réseau pour un réseau à filtrer.

Par exemple, pour filtrer sur 192.168.1.0/24 (255.255.255.0), on prendra un masque générique 0.0.0.255.

Autre exemple, pour filter sur 192.168.1.0/27 (255.255.255.224), on prendra un masque générique 0.0.0.31.

- Le mot "any" remplace le 0.0.0.0 255.255.255.255, autrement dit toute adresse IP
- Le mot "host" remplace le masque 0.0.0.0, par exemple, 10.1.1.1 0.0.0.0 peut être remplacé par "host 10.1.1.1"

2.10 Règles d'application

- Placer les listes d'accès aussi près de que possible de la source des paquets (au niveau de l'interface) s'il s'agit d'une ACL étendue. Par contre, s'il s'agit d'une ACL standard, il faut la placer au plus proche de la destination (puisque c'est ce qu'elle ne vérifie pas).
- Placer en tête de liste les règles (les instructions) qui font l'objet d'une correspondance la plus précise et les plus générales à la fin.
- Suivre ces deux recommandations tout en respectant les restrictions d'accès qui ont été identifiées.

2.11 Syntaxe des commandes

La mise en oeuvre d'une ACL se déroule en deux étapes :

2. Création de la liste, en plaçant les instructions les unes après les autres suivies d'un retour chariot.
3. Application sur une interface en entrée ou en sortie

Attention, on ne peut pas insérez une instruction dans une liste existante ni la modifiée. On ne peut qu'ajouter des instructions à la fin de la liste.

2.11.1 Liste d'accès standard

```
Router(config)#access-list numéro-liste-accès {deny|permit} adresse-source [masque-source] [log]
```

2.11.2 Liste d'accès étendue

```
Router(config)#access-list numéro-liste-accès {deny|permit} protocole adresse-source masque-source
[opérateur port] adresse-destination masque-destination [opérateur port] [log]
```

Où "opérateur" peut prendre les valeurs suivantes :

- lt (less than)
- gt (greater than)
- eq (equal)
- neq (not equal)
- range (inclusive range).

Où le paramètre "port" peut prendre une valeur nominative ou numéraire de 0 à 65535 ou, par exemple, http, telnet, ftp, etc.

2.11.3 Liste d'accès nommée

```
Router(config)#ip access-list standard nom
Router(config-ext-nacl)#permit|deny ...

Router(config)#ip access-list extended nom
Router(config-ext-nacl)#permit|deny ...
```

2.11.4 Activation d'une liste d'accès sur une interface

```
Router(config-if)#ip access-group {numéro-liste-accès|nom [in | out]}
```

2.11.5 Diagnostic

```
Router#show ip interface [type numéro]

Router#show access-lists [numéro-liste-accès|nom-liste-accès]

Router#show ip access-list [numéro-liste-accès|nom-liste-accès]
```

2.12 Plus d'informations

Ce cours a été élaboré à partir d'un article de François Goffinet, Instructeur Cisco :

http://cisco.goffinet.org/s2/c11

3 Prérequis

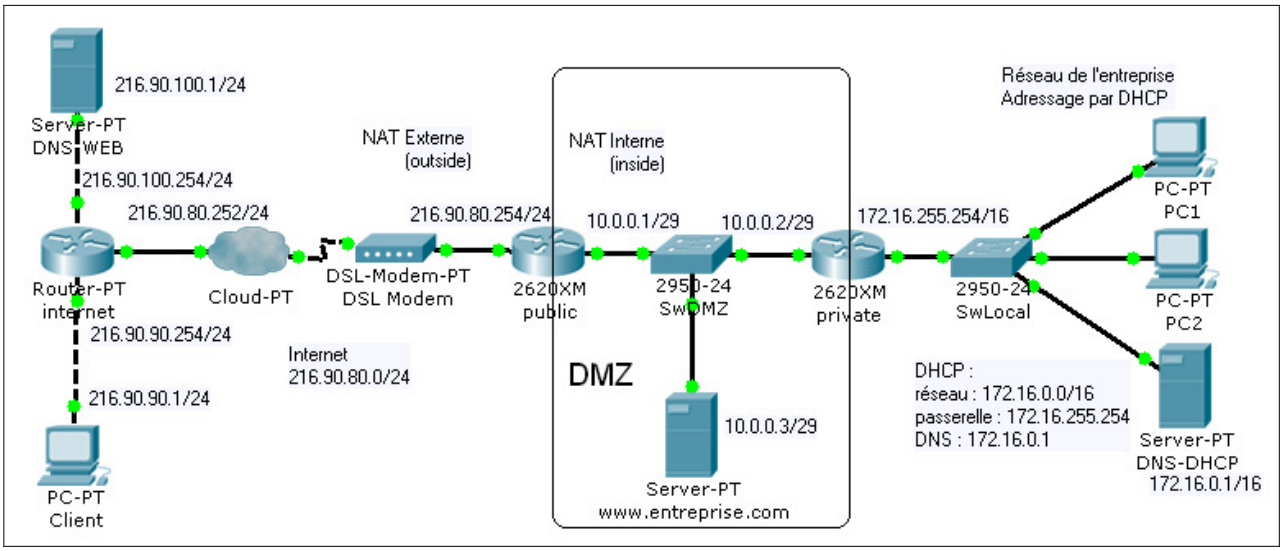
Pour réaliser ce TP, vous devez avoir fait les TP « Le matériel dans un réseau local TCP/IP », « Configuration des routeurs Cisco avec l'IOS » et « Liaisons WAN ».

Vous aurez besoin du logiciel Packet Tracer V4.1 de Cisco.

4 Travail a réaliser

4.1 Le réseau

Réalisez la structure de réseau suivante :



4.2 Routage et DNS

Appliquez à tous le routeur le protocole RIP.

Vérifiez que tous les postes et serveurs puissent communiquer entre eux.

Pinguez www.entreprise.com depuis Client : _____

Pour permettre de pinguez à partir des nom de domaine, les DNS doivent être renseignés :

- Client : DNS 216.90.100.1
- Réseau entreprise : DNS 172.16.0.1

En mode simulation (flitrez les protocoles ICMP et DNS), pinguez www.entreprise.com depuis Client puis, cliquez sur l'enveloppe du message final du protocole DNS (le rechercher dans la liste des événement et double-cliquer dessus pour faire apparaître l'enveloppe du message sur le schéma).

Consultez la partie DNS de la trame (Inbound PDU Details). Quelle est l'adresse renvoyée par le DNS ?

Ciquez sur l'enveloppe du message final ICMP. Quelles sont les adresses source et destination ?

4.3 Translation d'adresses

Pour protéger le réseau de l'entreprise et limiter le nombre d'adresses publiques à utiliser, on a recourt à la translation d'adresses privées en adresses publiques :

Vue de l'extérieur (internet), le réseau de l'entreprise a pour adresse 216.90.80.254 et son serveur web 216.90.80.253.

- Lors du passage d'une trame par le routeur « public » dans le sens private → public, les adresses privés (176.16.0.0) sont remplacées par l'adresse externe du routeur (216.90.80.254). L'adresse interne est stockée dans une table nat pour la remettre en place lors du retour de la trame.
- Lors du passage d'une trame par le routeur « public » dans le sens public → private, la seule adresse routable est celle du serveur web de l'entreprise (216.90.80.253). Elle est donc remplacée par son adresse interne (10.0.0.3) à l'allée et remise en place au retour.

Indiquez au routeur quelles sont ses interfaces interne et externe :

Interface interne	*Interface externe*
`Public(config)#`	`Public(config)#`

Ecrivez la règle de translation nat statique permettant de translater 10.0.0.3 en 216.90.80.253 :

```
Public(config)# ip nat _____________________________________________________________________
```

Pour permettre la translation des adresses du réseau 172.16.0.0 en l'adresse publique du routeur, il faut créer une règle de translation dynamique. Il faut créer une liste qui contient les adresses réseau à translater.

Créez une access-list standard numérotée 1 et permettant l'accès au réseau 172.16.0.0 :

```
Public(config)# access-list 1 _______________________________________________________________
```

Créez la règle de translation nat dynamique ayant pour source la liste 1 et pour adresse translatée, l'interface publique du routeur

```
Public(config)# ip nat _____________________________________________________________________
```

Procédez aux tests de connectivité consultez les trames pour observez la translation d'adresses.

Source	*Destination*	*Résultat – Adresses translatées*
PC1 ou 2	Client	
www.entreprise.com	Client	
Client	PC1 ou 2	
Client	www.entreprise.com	

La translation d'adresses à surtout pour but de cacher le réseau interne de l'extérieur mais si on connais le type d'adresses en vigueur dans le réseau, on peut peut toujours y accéder directement. Il faut donc protéger l'accès au réseau en appliquant des règles de filtrage. Le DNS d'internet (DNS-WEB) doit être mis à jour avec l'adresse translatée de www.entreprise.com.

4.4 Protection du réseau de l'entreprise.

Le réseau de l'entreprise doit être parfaitement hermétique à toute intrusion de l'extérieur. Cependant, les postes de ce réseau doivent toujours pouvoir accéder à internet.

On affectera donc à l'interface côté réseau d'entreprise, une liste de contrôle d'accès en entrée et en sortie :

En entrée :

- Autoriser tous les protocoles IP venant 172.16.0.0 vers tous les hôtes.

En sortie :

- Autoriser le protocole TCP en provenance du port 80 de tous les hôtes à destination du réseau 172.16.0.0 s'il s'agit de la réponse à une de ses requettes.
- Autoriser le protocole ICMP en provenance de la DMZ à destination du réseau d'entreprise
- Autoriser le protocole ICMP en provenance de tous les hôtes et à destination du réseau d'entreprise lorsqu'il s'agit d'une réponse à une de ses requettes.

Le protocole ICMP est utile pour tester la connectivitée et s'assuré que les problèmes éventuels ne sont pas liés au câblage, à l'alimentation des hôtes ou routage. Cependant, on autorisera seulement son utilisation depuis le réseau de l'entreprise ou depuis la DMZ.

Ecrivez les listes de contrôle d'accès correspondantes :

En entrée ACL 101	`private(config)# access-list 101`
En sortie ACL 100	`private(config)# access-list 100`

Activez les listes sur l'interface du routeur :

```
private(config)#
```

Procédez aux tests de connectivité consultez les trames au passage du routeur «`private`». Vérifiez l'application des règles de filtrages.

Source	*Destination*	*Résultat – Adresses translatées*
PC1 ou 2	Client	
www.entreprise.com	Client	
Client	PC1 ou 2	
Client	www.entreprise.com	

En mode simulation, filtrez les protocoles DNS et HTTP.

Depuis le navigateur web de PC1 ou PC2, entrez l'adresse des sites web www.entreprise.com et www.siteweb.com. Vérifiez la possibilité d'accéder aux deux sites web.

4.5 Protection de la DMZ

La DMZ est accessible depuis internet pour tous les protocoles. Or celle-ci n'héberge qu'un serveur web. Le seul protocole qui devrait être autorisé à la pénétrer est le HTTP soit les requettes TCP a destination du port 80 du serveur web de l'entreprise.

Cependant, il ne faut pas oublier que les hôtes du réseau de l'entreprise doivent pouvoir accéder à internet. Il faut donc laisser passer tous le trafic tcp en provenance d'un port 80 lorsqu'il s'agit d'une réponse.

Notons aussi que les routeurs entretiennent leur table de routage automatiquement grâce au protocole RIP. Le routeur « public » doit pouvoir propager ce protocole vers les autres routeurs et l'accepter des autres routeurs. Comme il n'est pas directement possible de filtrer RIP, on filtrera les protocoles IP en entrée lorsque la source des trames est l'interface de sortie du routeur « internet ».

Pour assurer l'administration du réseau, on autorisera aussi le protocole ICMP lorsqu'il s'agit d'une réponse et lorsque la destination est l'adresse de substitution du serveur web de l'entreprise.

Vous numéroterez cette liste de contrôle d'accès 111 et vous l'appliquerez à l'interface d'entrée de la DMZ (côté internet) :

```
public(config)#
```

Effectuez les tests de connectivité et vérifiez les trames au passage du routeur « public ».

Procédez aux tests de connectivité consultez les trames au passage du routeur «`private`». Vérifiez l'application des règles de filtrages.

Source	*Destination*	*Résultat*
PC1 ou 2	Client	
www.entreprise.com	Client	
Client	PC1 ou 2	
Client	www.entreprise.com	

En mode simulation, filtrez les protocoles DNS et HTTP.

Depuis le navigateur web de PC1 ou PC2, entrez l'adresse des sites web www.entreprise.com et www.siteweb.com. Vérifiez la possibilité d'accéder aux deux sites web.

Faites la même chose depuis Client.

Pour vérifier l'hermétisme aux autres protocoles, modifiez la référence au DNS de Client par 216.90.80.253 et refaites depuis le navigateur de client une tentative d'accès à www.entreprise.com.

Consultez la trame au passage du routeur « public ». Quelle règle s'est appliquée ?

4.6 Conclusion

Le serveur web de l'entreprise devra aussi héberger un serveur ftp. Quelles sont les règles à ajouter ?