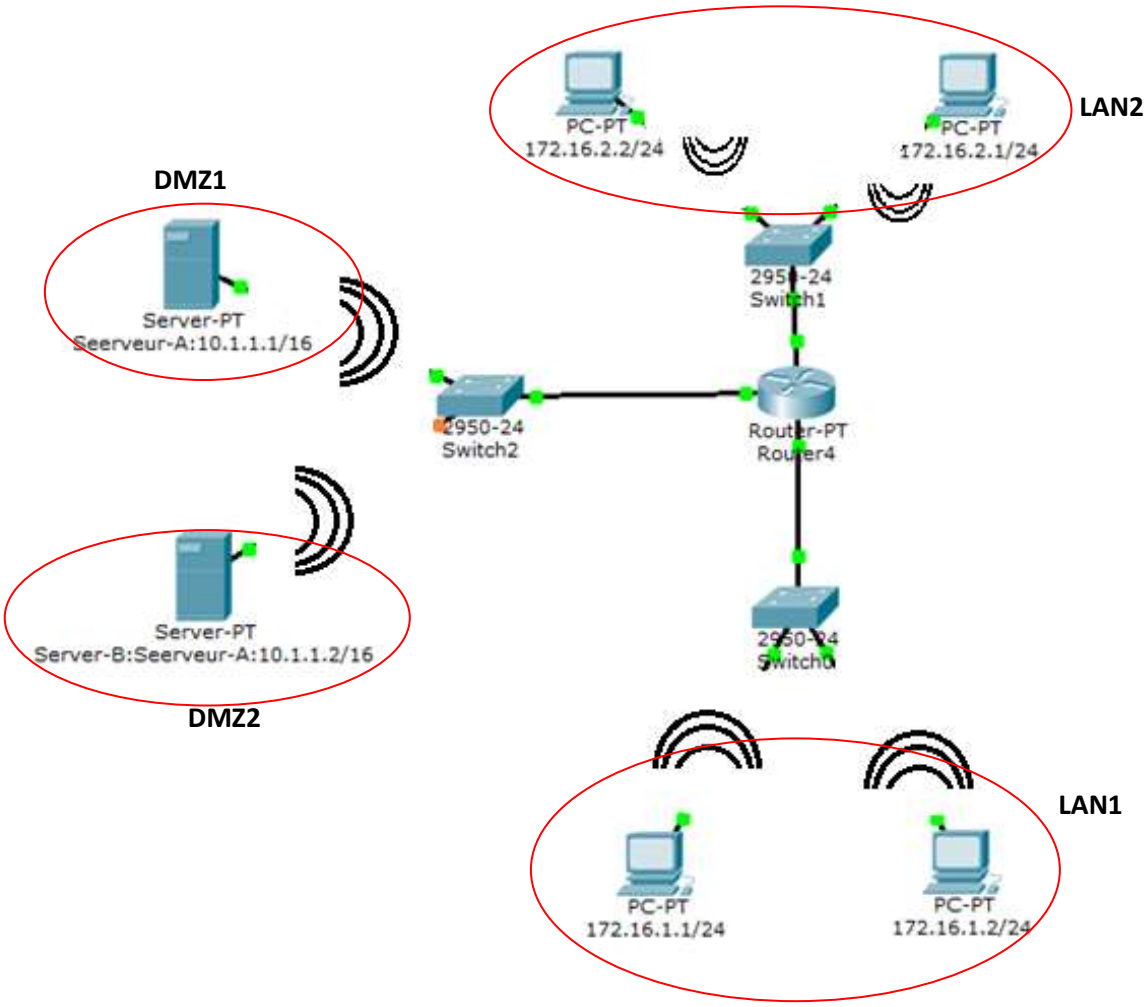
Université Dr Tahar Moulay de Saida
Faculté de Technologie
Département d'informatique

CSTRSF TP N°2 : Filtrage, ACL, Par feu



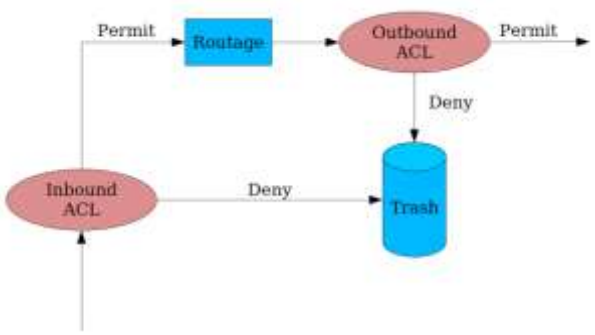
1. On veut bloquer l'accès du réseau 172.16.1.0 au serveur A
2. On veut bloquer l'accès du poste 172.16.2.2 au serveur A
3. On veut bloquer l'accès HTTP du réseau 172.16.2.0 au serveur A
4. On veut bloquer tout accès ICMP du réseau 172.16.2.0 au serveur B
5. On veut bloquer le *ping* du poste 172.16.1.1 au serveur B
6. On veut bloquer l'accès au poste 172.16.2.1
7. On veut bloquer l'accès au poste 172.16.1.2 par le poste 172.16.2.2

Annexe : Access Control Lists

Les ACL ?

- Une ACL est une liste de règles permettant de filtrer (Autoriser, bloquer ou rejeter) des paquets suivant des critères déterminés par l'utilisateur Sur des paquets IP en fonction : de l'IP source, de l'IP destination, …

Schéma du principe



Configuration d'une ACL numérique standard

- Définition d'une règle
  - ✓ **access-list** *number* [**deny | permit**] *source* [source-wildcard]
    Remarque : Nombre compris entre 1 et 99 ou entre 1300 et 1999
  - ✓ **access-list** number **remark** test
- Activation d'une ACL sur une interface
  - ✓ **ip access-group [** number | name **[in | out]]**
- Visualiser les ACL
  - ✓ **show access-lists:** toutes les ACL quelque soit l'interface
  - ✓ **show ip access-lists** [number | name **] :** les ACL uniquement liés au protocole IP
- Supprimer une ACL
  - ✓ **no access-list** [number | name **]**
- Modifier une ACL
  - ✓ **ip access-list [standard|extended]** [number | name **]**
  - ✓ **no** [Numéro de règle **]**
  - ✓ [**Numéro de règle]** [**deny | permit**] *addr* [source-wildcard]
- Configuration d'une ACL nommée standard
  - ✓ **ip access-list [standard|extended] monACL**
  - ✓ [**deny | permit**] *addr* [source-wildcard]
- Vérification des ACLs appliquées sur une interface
  - ✓ **show ip interface fastEthernet 0/0**

Exemple 1:

- **access-list 1 deny** 172.16.2.1 0.0.0.0
  - ✓ Refuse les paquets d'IP source 172.16.2.1
  - ✓ Le masque (également appelé wildcard mask) signifie ici que tous les bits de l'adresse IP sont significatifs
- **access-list 1 permit** 0.0.0.0 255.255.255.255
  - ✓ Tous les paquets IP sont autorisés
  - ✓ Le masque 255.255.255.255 signifie qu'aucun bit n'est significatif

Exemple 2:

```
access-list 1 remark stop tous les paquets d'IP source 172.16.3.10
access-list 1 deny host 172.16.3.10
access-list 1 permit any
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out
```

Exemple 3:

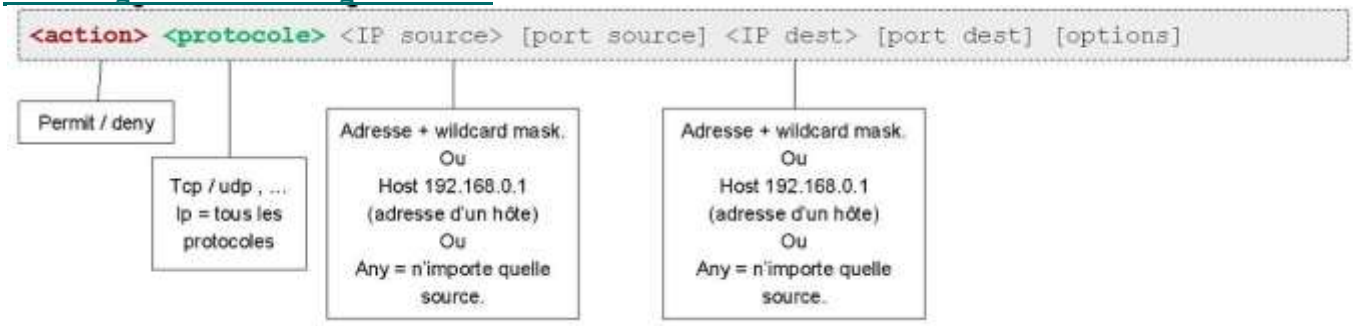
```
interface Ethernet0
ip address 172.16.1.1 255.255.255.0
ip access-group 1 out
interface Ethernet1
ip address 172.16.2.1 255.255.255.0
ip access-group 2 in
access-list 1 remark Stoppe tous les paquets d'IP source 172.16.3access-list 1 deny host 172.16.3.10
access-list 1 permit any
access-list 2 remark Autorise que les trames d'IP source 172.16.3
access-list 2 permit 172.16.3.0 0.0.0.255
```

- Une notation améliorée est possible pour remplacer
  - ✓ le masque 255.255.255.255 qui désigne une machine
    - Utilisation du terme **host**
  - ✓ avec le wildcard masque à 255.255.255.255 qui désigne tout le monde
    - Utilisation du terme **any**

Les extended ACL

- Les ACLs étendues permettent filtrer des paquets en fonction
  - ✓ de l'adresse de destination IP
  - ✓ Du type de protocole (TCP, UDP, ICMP, IGRP, IGMP, ...)
  - ✓ Port source
  - ✓ Port destination
  - ✓ ...

Format général d'une règle étendue



La syntaxe et exemple

- **access-list** *number* { **deny** | **permit** } *protocol source source-wildcard destination dest-wildcard*
  - ✓ *number* : compris entre 100 et 199 ou 2000 et 2699
- **access-list 101 deny ip any host 10.1.1.1**
  - ✓ Refus des paquets IP à destination de la machine 10.1.1.1 et provenant de n'importe quelle source
- **access-list 101 deny tcp any gt 1023 host 10.1.1.1 eq 23**
  - ✓ Refus de paquet TCP provenant d'un port > 1023 et à destiantion du port 23 de la machine d'IP 10.1.1.1
- **access-list 101 deny tcp any host 10.1.1.1 eq http**
  - ✓ Refus des paquets TCP à destination du port 80 de la machine d'IP 10.1.1.1

Les ACL nommés

- Une ACL numéroté peut être composé de nombreuses règles. La seule façon de la modifier et de faire
  - ✓ **no access-list** *number*

- ✓ Puis de la redéfinir

- Avec les ACL nommées, il est possible de supprimer qu'une seule ligne au lieu de toute l'ACL
- Sa définition se fait de la manière suivante
  - ✓ **Router(config)# ip access-list extended bart**
  - ✓ **Router(config-ext-nacl)# deny tcp host 10.1.1.2 eq www any**
  - ✓ **Router(config-ext-nacl)# deny ip 10.1.1.0 0.0.0.255 any**
  - ✓ **Router(config-ext-nacl)# permit ip any any**
- Pour supprimer une des lignes, il suffit de refaire un
  - ✓ **ip access-list extended bart**
  - ✓ **Puis un no deny ip 10.1.1.0 0.0.0.255 any**