ACL CISCO avancée

Notion de masque générique (wildcard mask)

Les ACL utilisent un masque permettant de sélectionner des plages d'adresses.

En binaire, seuls les bits de l'adresse qui correspondent au bit à 0 du masque sont vérifiés.

L'exécution d'une opération **OU** sur le réseau entraîne la plage d'adresses IP (192.168.248.96-103) qui peut être autorisée ou bloquée dans une déclaration de réseau ACL ou OSPF

Le travail d'un masque de sous-réseau consiste à séparer les bits d'hôte des bits de réseau. Le nombre de 1 dans le masque de sous-réseau **doit être contigu** .

Les masques génériques ne sont pas liés par cette règle, vous pouvez donc faire des masques de ce type:

```
access-list 1 permit 192.168.200.0 0.6.0.8
```

Cela permettra aux réseaux suivants de fonctionner

192.168.200.0
192.172.200.0
192.168.200.8
192.172.200.8

ACL AVANCEE

Pour protéger le réseau LAN et/ou DMZ du trafic venant de l'extérieur, on est souvent obligé de bloquer tout trafic par défaut et n'autoriser que le strict nécessaire, mais cela

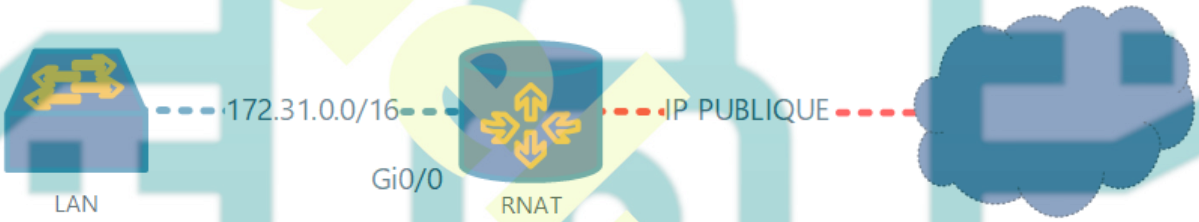
devient complexe à gérer notamment lorsque que l'on veut gérer les requêtes initiées de l'intérieur et autoriser les réponses associées de l'extérieur.

Nous avons à disposition la gestion des flags TCP (established…) la gestion d'ICMP (echo-reply…) et la gestion des ports UDP (supérieur à 1023)

L'inconvénient majeur, c'est que ce n'est pas très souple et sécurisé pour le protocole UDP.

Il existe d'autres méthodes comme le filtrage par Access-list **réflexive**, qui consiste à générer une ACL dynamiquement en fonction du trafic sortant afin d'autoriser le retour. On peut également utiliser les **Zone-Based Firewall** dont le principe est de définir des zones et de créer des règles entre les zones.

ACL réflexive



Etape 1 – Création de l'ACL autorisant le trafic sortant

```
RNAT(config)#ip access-list extended ACL-LANWAN
RNAT(config-ext-nacl)#permit ip 172.31.0.0 0.0.255.255 any reflect ACL-REFLECTED
```

ACL-L2W (Lan to Wan) sera l'ACL affectée sur l'interface côté LAN de RNAT en IN. On autorise le trafic IP provenant de 172.31.0.0/24 vers n'importe quelle direction. L'instruction **reflect** indique au routeur qu'il devra créer une règle réflexive (correspondant au trajet inverse) dans l'access-list dynamique ACL-REFLECTED.

Etape 2 – Création de l'ACL affectée sur l'interface côté LAN de RNAT en OUT.

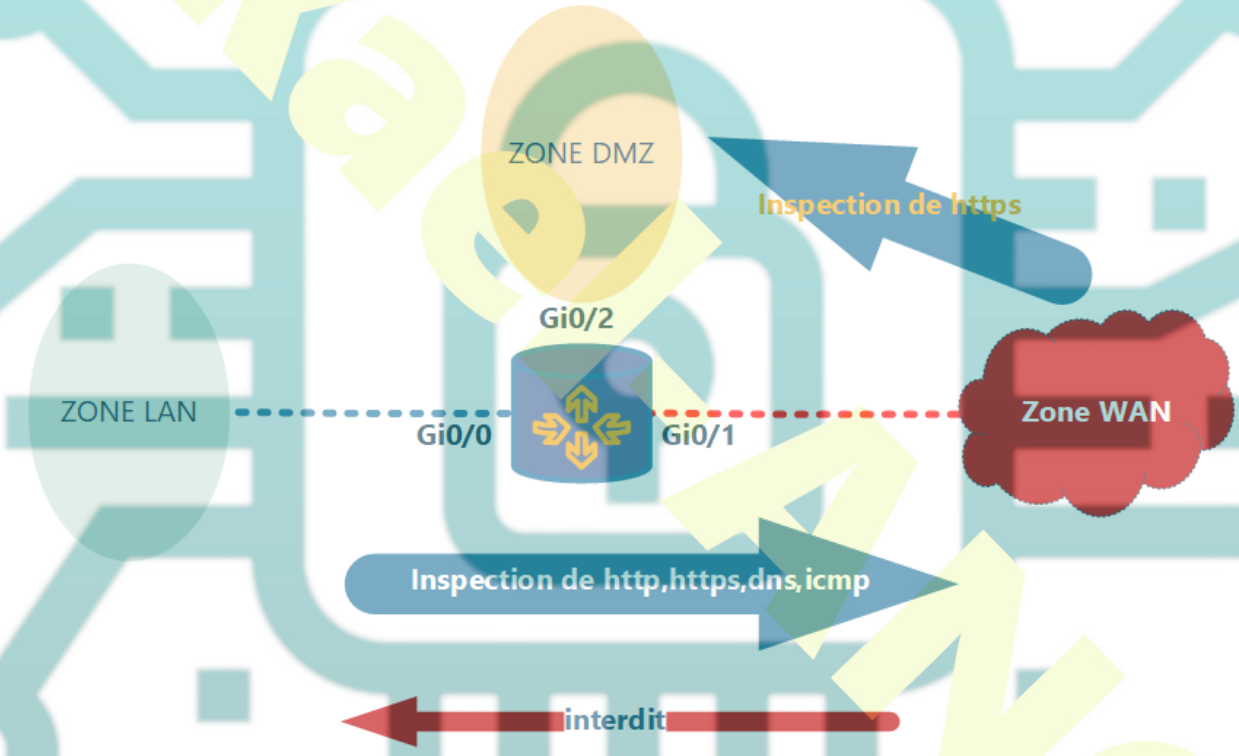
```
RNAT(config)#ip access-list extended ACL-WANLAN
RNAT(config-ext-nacl)#evaluate ACL-REFLECTED
```

ACL-WANLAN (Wan to Lan) ne contient ici qu'une seule instruction, **evaluate** ACL-REFLECTED, qui indique au routeur qu'il doit utiliser les règles contenues dans l'ACL ACL-REFLECTED.

Etape 3 – application des ACL sur l'interface LAN (gi0/0) de RNAT

```
RNAT(config)#int gi0/0
RNAT(config-if)#ip access-group ACL-LANWAN in
RNAT(config-if)#ip access-group ACL-WANLAN out
```

Zone-Based Firewall



Règle LAN-WAN

Etape 1 – création des Class-maps

```
class-map type inspect match-any internet-trafic-class
match protocol http
match protocol https
match protocol dns
match protocol icmp
```

Les Class-maps décrivent le trafic qui est permis entre les zones (selon la politique de sécurité)

- match-any demande correspondance sur n'importe quel critère.
- match-all demande correspondance sur tous les critères du Class-map.

Etape 2 – création de la Policy-map

```
policy-map type inspect internet-trafic-policy
class type inspect internet-trafic-class
inspect
```

Une Policy-map, reprend l'ensemble des critères de Class-maps

Etape 3 – Configuration des zones et assignation des interfaces

```
zone security lan
zone security internet
interface Gi0/0
zone-member security lan
interface Gi0/1
zone-member security internet
```

Étape 4 – configuration du lien "zone-pair" et application de la policy-map

```
zone-pair security lan-internet source lan destination internet
service-policy type inspect internet-trafic-policy
```

Règle WAN-DMZ

Etape 1 – création des Class-maps

```
class-map type inspect match-any internet-dmz-class
match protocol https
```

Etape 2 – création de la Policy-map

```
policy-map type inspect internet-dmz-policy
class type inspect internet-dmz-class
inspect
```

Etape 3 – Configuration de la zone et assignation de l'interface

```
zone security dmz
interface Gi0/2
zone-member security dmz
```

Étape 4 – configuration du lien "zone-pair" et application de la policy-map

```
zone-pair security internet-dmz source internet destination dmz
service-policy type inspect internet-dmz-policy
```

Dernière étape

Configuration des ACL classiques et des redirections NAT

VACL – ACL de VLAN

Les VACL contrôlent l'accès au VLAN de tous les paquets (pontés et routés). Les paquets peuvent entrer dans le VLAN via un port de couche 2 ou via un port de couche 3 après avoir été routés. Vous pouvez également utiliser les VACL pour filtrer le trafic entre les périphériques du même VLAN.

De manière générale, une VACL fonctionne sur un principe similaire à celui des route-maps. Il s'agit d'une liste ordonnée de règles, chacune ayant un numéro de séquence. Pour chacune de ces règles nous devons identifier le trafic correspondant à l'aide d'une clause « match », à laquelle nous ferons correspondre une « action » qui peut être l'une des trois suivantes:

- **forward**: le trafic est traité normalement en suivant la logique de commutation du switch.

- **drop**: le trafic est rejeté.
- **redirect**: le trafic est redirigé vers une interface spécifique, indépendamment de la logique de commutation du switch.

Les clauses « match » utilisent des ACL (soit IP, soit MAC).

Les VACL rejettent tout ce qui n'est pas permis. Une VACL sans règle « forward » bloquera tout simplement tout le trafic dans le vlan donné.

ACL VLAN

Les ACL VLAN (VACL) peuvent fournir un contrôle d'accès pour tous les paquets qui sont pontés dans un VLAN ou qui sont acheminés vers ou hors d'un VLAN.

Contrairement aux listes de contrôle d'accès Cisco IOS qui sont appliquées uniquement aux paquets routés, les listes de contrôle d'accès VACL s'appliquent à tous les paquets et peuvent être appliquées à n'importe quelle interface VLAN.

Si un VACL est configuré pour un type de paquet et qu'un paquet de ce type ne correspond pas au VACL, l'action par défaut est de refuser le paquet.

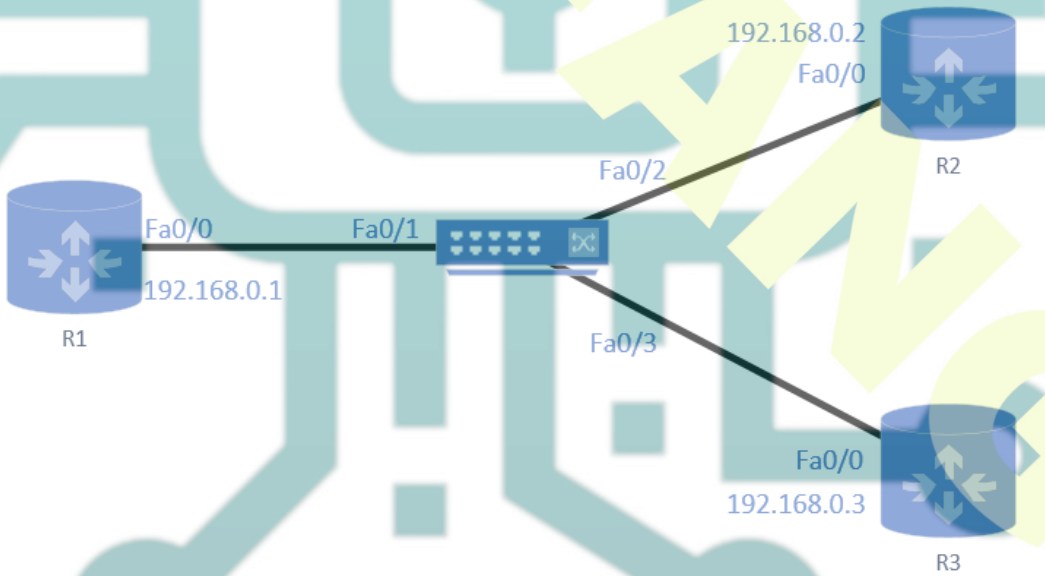


Schéma de l'exemple

Sans VACL, les trois routeurs peuvent communiquer entre eux sans problème, nous allons faire en sorte que R1 puisse communiquer avec R2 et R3 mais que R2 et R3 ne puissent

pas communiquer entre eux.

```
vlan 10
int range fa0/1 – 24
switchport access vlan 10
On crée une ACL étendue classique
ip access-list extended VLAN10
permit ip host 192.168.0.2 host 192.168.0.3
permit ip host 192.168.0.3 host 192.168.0.2
```

1. On crée une Vlan Access Map qui combine les matches avec les actions, munie de deux règles.
2. Le trafic correspondant à l'ACL VLAN10 doit être « droppé » (**n° de séquence 10**)
3. Le reste du trafic doit être « forwardé » (**n° de séquence 20**)

```
vlan access-map VMAP-VLAN10 10
match ip address VLAN10
action drop
vlan access-map VMAP-VLAN10 20
action forward
On applique la VACL au VLAN
vlan filter VMAP-VLAN10 vlan-list 10
```

L'exemple suivant montre une VACL appliquée au VLAN 10 pour éliminer le trafic ICMP, et autoriser tout autre trafic.

NB. L'ACL nommées PING contient uen entrée avec l'action "permit" car elle ne sert que de critère de correspondance à l'access map qui les filtre par l'action drop.

```
ip access-list extended PING
permit icmp any any
ip access-list extended OTHER
permit ip any any
vlan access-map VACL_10 10
match ip address PING
```

```
action drop
vlan access-map VACL_10 20
match ip address OTHER action forward
vlan filter VACL_10 vlan-list 10
```

PACL – ACL des ports

La fonction ACL de port (PACL) permet d'effectuer un contrôle d'accès sur des ports de couche 2 spécifiques.
Un port de couche 2 est un LAN physique ou un port de jonction qui appartient à un VLAN.

Les listes de contrôle d'accès de port sont appliquées uniquement au trafic entrant.

La fonction ACL de port n'est prise en charge que par le matériel (les ACL de port ne sont appliquées à aucun paquet acheminé dans le logiciel).

Les ACL de port effectuent un contrôle d'accès sur tout le trafic entrant dans le port de couche 2 spécifié.

Création d'une une liste d'accès MAC

```
(config)# mac access-list extended acl-name
(config-ext-macl)# permit [ host source-mac | any ] [ host dest-mac | any ]
```

Appliquer au port

```
interface interface-id
match access-group acl – name in
```

Ordre d'exécution des ACL

L'ordre du filtrage du trafic "ponté" (au sein du même VLAN) est le suivant :

- PACL en entrée sur un switchport
- VACL en entrée sur le VLAN
- VACL en sortie sur le VLAN

L'ordre du filtrage du trafic "routé" (à travers les VLAN) est le suivant :

- PACL en entrée sur le switchport
- VACL en entrée sur le VLAN
- ACL en entrée sur la SVI
- ACL en sortie sur la SVI
- VACL en sortie sur le VLAN