Filtrage ACL Cisco

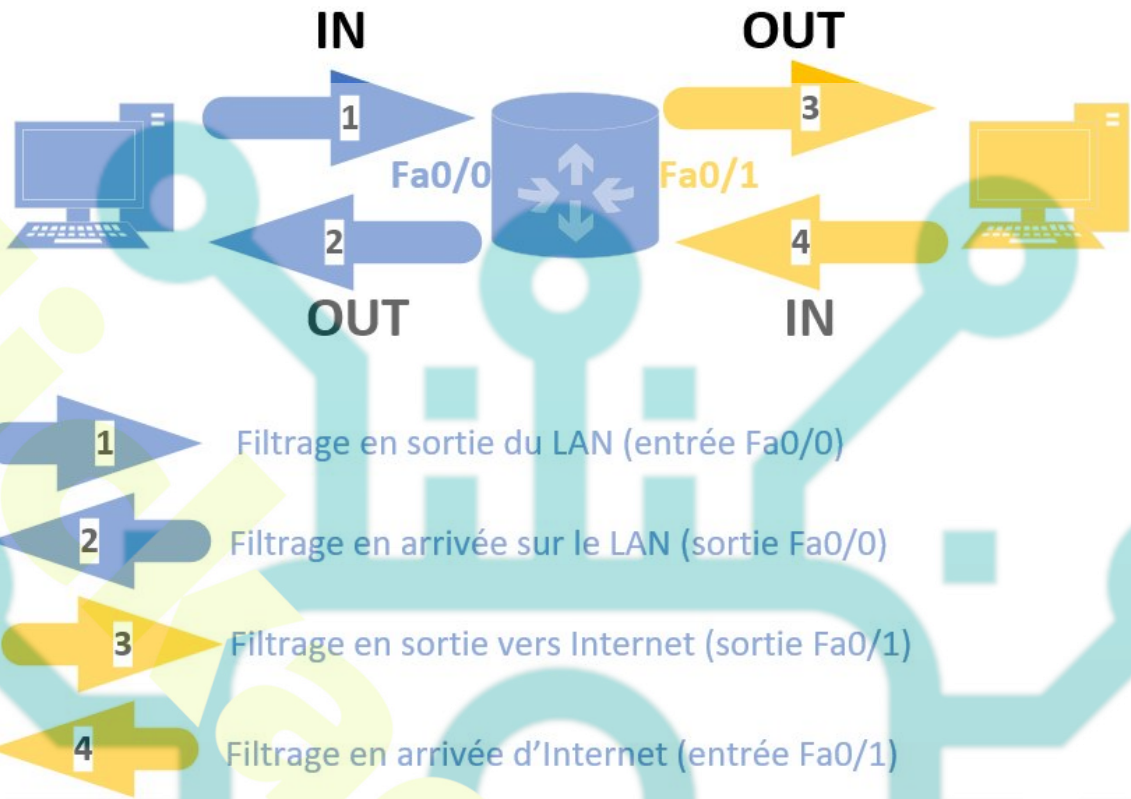
ACL

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

La configuration des ACLs IPv4 et des ACLs IPv6 sont similaires mais aussi très différentes.

Cette fonctionnalité Cisco IOS est utile pour :

- les fonctions de pare-feu
- le marquage du trafic, QoS
- les configurations NAT
- le contrôle des logs
- le contrôle des accès aux consoles virtuelles (VTY)
- le contrôle des informations de routage
- le contrôle du trafic SNMP, …



Positionnement ACL

Applications des ACL

Les ACL peuvent être appliquées sur le trafic entrant ou sortant. Il y a deux actions : **soit le trafic est interdit, soit le trafic est autorisé.**

Les ACL sont prises en compte de façon séquentielle. Il faut donc placer les instructions les plus précises en premier et l'instruction la plus générique en dernier.
Par défaut, tout le trafic est interdit.

Deux types d'ACLs (IPv4)

Les deux types d'ACLs se distinguent *en fonction des critères utilisés* :

Une liste simple (**standard**) et l'autre plus complexe (**étendue**) .

Note
Les ACLs standard n'existent plus en IPv6.

ACL standard

L'ACL standard **filtre uniquement sur les adresses IP sources.**
Le numéro de l'ACL standard est compris entre **1 et 99** ou entre **1300 et 1999**.

Exemple
R1(config)#access-list 10 permit 192.168.2.0 0.0.0.255
Cette ACL va permettre d'accepter le trafic venant du réseau ayant l'IP 192.168.2.0
R1(config)#access-list 20 deny host 192.168.2.4
Cette ACL va permettre de bloquer le trafic venant de l'hôte ayant l'IP 192.168.2.4 et uniquement de lui.

ACL étendue

Contrairement aux ACL standards, les ACL étendues ne se reposent pas uniquement sur l'adresse IP source, mais sur plusieurs champs de l'en-tête IP et sur les protocoles utilisés.

Les ACL étendues se placent au plus proche de la source (afin d'éviter de gaspiller de la bande passante en envoyant sur le réseau des paquets qui seront supprimés une fois arrivés à destination)

le protocole peut être :
<0-255> An IP protocol number
AHP Authentication Header Protocol
EIGRP Cisco's EIGRP routing protocol
ESP Encapsulation Security Payload
GRE Cisco's GRE tunneling
ICMP Internet Control Message Protocol
IGMP Internet Gateway Message Protocol
IP Any Internet Protocol
IPINIP IP in IP tunneling
OSPF OSPF routing protocol
TCP Transmission Control Protocol
UDP User Datagram Protocol

Quelques opérateurs

eq : égal
neq : différent
gt : plus grand que
lt : moins grand que

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.

1. avec 172.16.2.0 0.0.255.255, la partie vérifiée par le routeur sera 172.16
2. avec 0.0.0.0, toutes les adresses sont concernées (any)
3. avec 192.168.2.3 255.255.255.255, on vérifie uniquement l'hôte ayant l'IP 192.168.2.3 (host)

Donc, 0.0.0.255 correspond à un masque normal en /24 ou 255.255.255.0
0.0.255.255 correspond à un masque normal en /16 ou 255.255.0.0

Pour calculer rapidement le wildcard mask d'un sous réseau le plus simple est de faire une simple soustraction comme suit :

Exemple avec un masque /26

255.255.255.255
– 255.255.255.192
_____
= 0 . 0 . 0 . 63

Autre exemple pour un masque en /19

255.255.255.255
– 255.255.224. 0
_____
= 0 . 0 . 31. 255

Tableau récapitulatif des correspondances d'octets MASK / W.MASK

Octet Masque Normal	Octet Wilcard Mask	4ème Octet	3ème Octet	2ème Octet
255	0	/32	/24	/16
254	1	/31	/23	/15
252	3	/30	/22	/14
248	7	/29	/21	/13
240	15	/28	/20	/12
224	31	/27	/19	/11
192	63	/26	/18	/10
128	127	/25	/17	/9
0	255	/24	/16	/8

Les masques génériques sont également utilisés pour spécifier des sous-réseaux source / destination (ou des adresses spécifiques) dans les listes de contrôle d'accès.

```
IP:   1100 0000 . 1010 1000 . 1111 1000 . 0110 0100 =
192.168.248.100
Mask: 1111 1111 . 1111 1111 . 1111 1111 . 1111 1000 =
255.255.255.248
AND:  1100 0000 . 1010 1000 . 1111 1000 . 0110 0000 =
192.168.248.96
```

L' opération **ET** sur l'adresse IP avec le masque de réseau entraîne le réseau 192.168.248.96/29.

Ensuite, un caractère générique:

```
NET:  1100 0000 . 1010 1000 . 1111 1000 . 0110 0000 =
192.168.248.96
WC:   0000 0000 . 0000 0000 . 0000 0000 . 0000 0111 = 0.0.0.7
OR:   1100 0000 . 1010 1000 . 1111 1000 . 0110 0111 =
192.168.248.103
```

Les ACL nommées

On peut nommer des ACL standards et étendues. Le fait de nommer une ACL permet de les gérer plus facilement.

Écrire une ACL nommée standard

(config)#ip access-list standard **DENY192**
(config-std-nacl)#deny 192.168.1.0 0.0.0.255
(config-std-nacl)#permit any

Ecrire une ACL nommée étendue

(config)#ip access-list extended **PERMITLAN2LAN3**
permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

Affichage de la liste de contrôle

#show access-lists
#show ip access-lists

Suppression d'une ACL

(config)#no ip access-list extended **PERMITLAN2LAN3**

Comment appliquer les ACL ?

On crée l'ACL, ensuite on applique l'ACL à une interface en entrée ou en sortie (IN ou OUT) .

IN est utilisé pour les paquets entrants vers le Cisco, OUT est utilisé pour les paquets sortants du Cisco.

Suppression de l'association ACL/interface

```
(config)#int fa1/1
(config-if)#no ip access-group PERMITLAN2LAN3 out
```

Exemple d'ACL de routeur

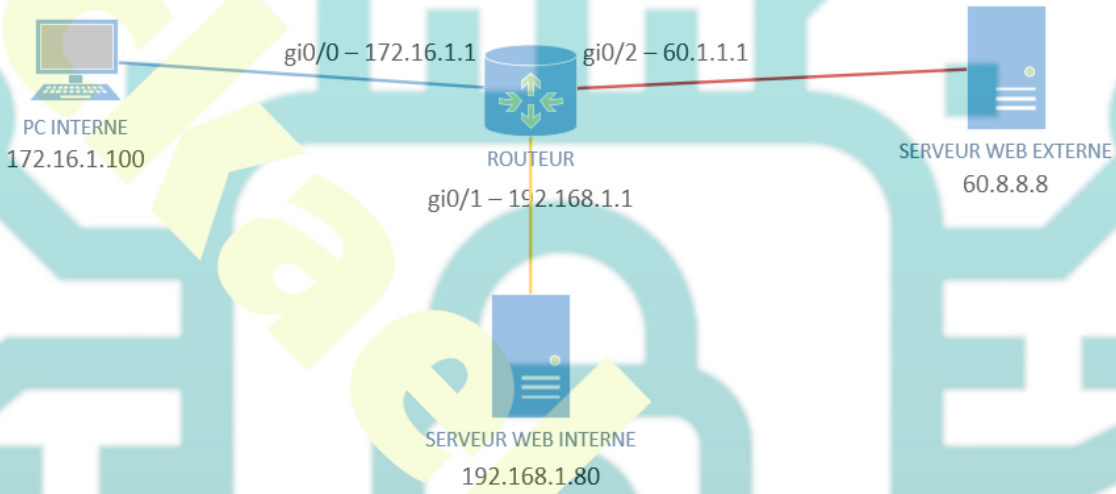


Schéma de test ¢ ACL routeur

Autoriser l'accès au réseau distant pour un réseau interne

Le trafic du PC interne 172.16.1.100 est autorisé vers l'extérieur pour toutes les requêtes vers le serveur 60.8.8.8 et le trafic du réseau interne 172.16.0.0 est autorisé vers l'extérieur uniquement en http et https.

```
Routeur(config)#ip access-list extended LAN-WAN
permit ip host 172.16.1.100 host 60.8.8.8 any
permit tcp 172.16.0.0 0.0.255.255 any eq 80
permit tcp 172.16.0.0 0.0.255.255 any eq 443
```

Affectation de la règle

```
Routeur (config)#int gi0/0
Routeur (config-if)#ip access-group LAN-WAN in
```

Par défaut, tout ce qui n'est pas explicitement autorisé est refusé. En fait, une clause implicite de refus se trouve à la fin de chaque ACL

Autoriser l'accès depuis internet au serveur web interne en https uniquement.

```
Routeur(config)#ip access-list extended WAN-DMZ
permit tcp any host 192.168.1.80 eq 443
Affectation de la règle
Routeur(config)#int gi0/1
Routeur(config-if)#ip access-group WAN-DMZ out
```

Refuser l'accès d'un réseau externe vers le réseau local

Le trafic de l'hôte 8.8.8.8 à destination de tous les réseaux internes est interdit.

```
Routeur(config)#ip access-list extended EX-NET
deny ip 80.0.0.0 0.255.255.255 any
R1(config)#int g0/2
R1(config-if)#ip access-group EX-HOST in
```

Exemple ACL de switch de niveau 3 avec VLAN

Schéma de test ¢ ACL switch

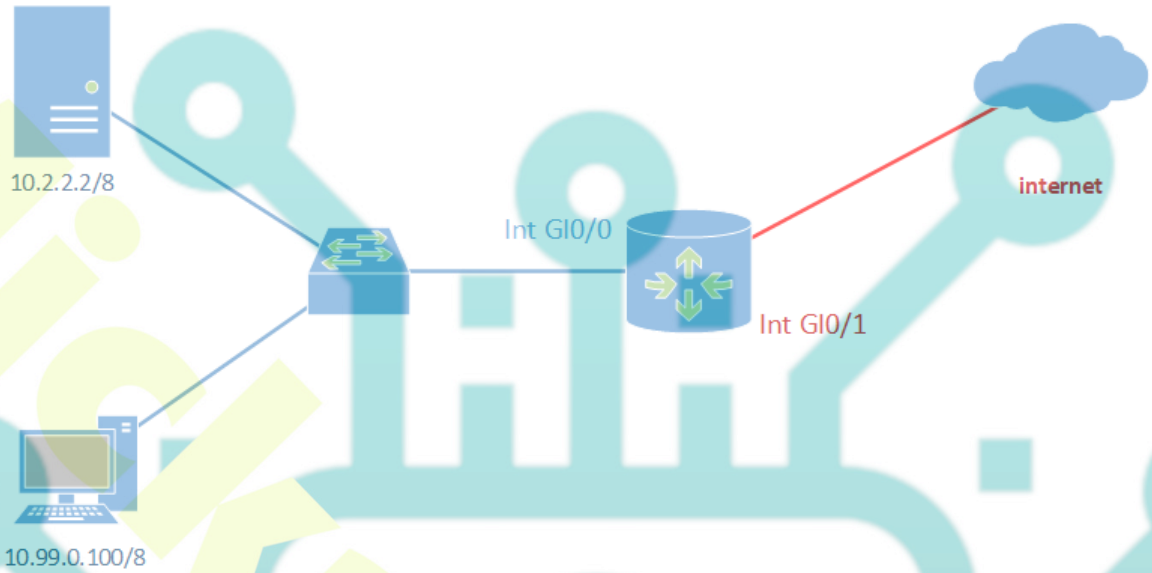
Empêcher le vlan 10 de communiquer avec le vlan 20

ip access-list extended V10-20
deny ip 10.10.0.0 0.0.255.255 10.20.0.0 0.0.255.255
On créer la règle autorisant au vlan 10 de communiquer avec les autres réseaux
permit ip any any
On affecte la règle en IN
int vlan10
ip access-group V10-20 in

Empêcher le vlan 20 de communiquer avec le vlan 10

ip access-list extended V20-10
deny ip 10.20.0.0 0.0.255.255 10.10.0.0 0.0.255.255
On créer la règle autorisant au vlan 20 de communiquer avec les autres réseaux
permit ip any any
On affecte la règle en IN
int vlan20
ip access-group V20-10 in

Autoriser uniquement les réponses depuis l'extérieur



Autoriser le routeur à laisser passer les réponses à un ping

Le réseaux local doit pouvoir faire un ping vers internet, mais internet ne doit pas être autorisé à faire un ping vers ce réseau, seule la réponse au echo-request est autorisée.

```
ip access-list extended reply_icmp
permit icmp any 10.0.0.0 0.255.255.255 echo-reply
interface gi0/0
ip access-group reply_icmp out
```

NB. on pourrait placer cette règle sur l'interface gi0/1 mais en IN cette fois-ci. Cependant, la règle n'est pas au plus proche de l'élément que l'on veut protéger.

Autoriser le routeur à laisser passer les requêtes TCP depuis le réseau LAN

Le réseau local doit pouvoir faire des connexions TCP vers internet, mais internet ne doit pas être autorisé à faire des requêtes TCP vers ce réseau, seule la réponse à la connexion établie est autorisée.

```
ip access-list extended tcp_connect
permit tcp any 10.0.0.0 0.255.255.255 established
```

On affecte l'ACL à l'interface en OUT

```
interface gi0/0
ip access-group tcp_connect out
```

Filtrer les connexions SSH avec les ACL

Dans la commande suivante, la liste de contrôle d'accès autorise uniquement au PC 10.99.0.100 à se connecter en ssh au routeur.

```
access-list standard SSH
permit tcp host 10.99.0.100 any eq 22
deny any
```

On autorise la connexion exclusive de ce réseau sur les terminaux virtuel

```
(config)#line vty 0 15
(config-line)#access-class SSH in
```