Les ACL (Access Control Lists)

Cours rédigé par : GADONNAUD Ewen

Formation : BTS SIO 1ère année - Option SISR

Établissement : Lycée Paul-Louis Courier, Tours

Date : Mars 2026

1. Qu'est-ce qu'une ACL ?

Une ACL (Access Control List) est un ensemble de règles appliquées sur une interface d'un routeur ou switch L3 pour **filtrer le trafic réseau**. Chaque règle (appelée ACE — Access Control Entry) autorise ou refuse des paquets selon des critères définis.

À quoi ça sert ?

- Bloquer l'accès d'un VLAN vers un autre
- Autoriser uniquement certains protocoles ou ports
- Restreindre l'accès à des ressources sensibles (serveurs, équipements réseau)
- Limiter le trafic entrant depuis Internet

2. Fonctionnement

Traitement séquentiel

Les règles d'une ACL sont lues **dans l'ordre**, de haut en bas. Dès qu'une règle correspond au paquet, elle est appliquée et les suivantes sont ignorées.

```
Paquet entrant
      |
      v
  Règle 1 → correspond ? → OUI → Action (permit/deny) → FIN
      |
      NON
      |
  Règle 2 → correspond ? → OUI → Action (permit/deny) → FIN
      |
```

```
    NON
     |
Règle 3 ...
     |
    NON
     |
deny any implicite → Paquet bloqué
```



Toute ACL se termine par un **deny any implicite invisible**. Si aucune règle ne correspond au paquet, il est bloqué. Il faut toujours ajouter un `permit any` explicite en fin d'ACL si on veut autoriser le reste du trafic.

Direction d'application

Une ACL s'applique sur une interface dans une direction :

Direction	Signification
in	Filtre le trafic **entrant** sur l'interface (avant le routage)
out	Filtre le trafic **sortant** de l'interface (après le routage)

3. Types d'ACL

Type	Numéros	Critères de filtrage
Standard	1-99 / 1300-1999	IP source uniquement
Étendue	100-199 / 2000-2699	IP source, IP destination, protocole, port

ACL Standard — simple mais peu précise. Elle filtre uniquement sur l'adresse IP source, sans tenir compte de la destination ni du protocole.

ACL Étendue — plus fine. Elle permet de filtrer sur la combinaison source + destination + protocole + port, ce qui la rend adaptée à la majorité des cas réels.



Toujours préférer les **ACL nommées** aux ACL numérotées. Elles sont plus lisibles, plus faciles à modifier, et permettent de supprimer une règle précise sans recréer toute l'ACL.

4. Placement des ACL

Le placement est critique : une ACL mal placée peut bloquer du trafic légitime ou laisser passer du trafic indésirable.

Type	Règle de placement	Raison
Standard	Au plus près de la **destination**	Elle ne filtre que sur la source — placée trop près de la source, elle bloquerait l'accès à tous les réseaux

Type	Règle de placement	Raison
Étendue	Au plus près de la **source**	Elle est précise (src + dst + port) — l'y placer évite que le trafic indésirable traverse inutilement le réseau

5. Maquette de référence

On réutilise la maquette de la page VLANs :

```
  VLAN 10 – USERS     → 192.168.10.0/24  (passerelle : 192.168.10.1)
  VLAN 20 – IT        → 192.168.20.0/24  (passerelle : 192.168.20.1)
  VLAN 30 – SERVEURS  → 192.168.30.0/24  (passerelle : 192.168.30.1)

  Serveur Web : 192.168.30.10 (HTTP/HTTPS)
  Serveur SSH : 192.168.30.20 (port 22)
```

6. ACL Standard — Exemple

Objectif : Interdire au VLAN 10 (USERS) d'accéder au VLAN 20 (IT).

Placement : proche de la destination → sur l'interface du routeur côté VLAN 20, en **out**.

```
ROUTEUR(config)# ip access-list standard BLOC-USERS-VERS-IT
ROUTEUR(config-std-nacl)# deny   192.168.10.0 0.0.0.255
ROUTEUR(config-std-nacl)# permit any

ROUTEUR(config)# interface GigabitEthernet0/0.20
ROUTEUR(config-subif)# ip access-group BLOC-USERS-VERS-IT out
```

Lecture de la règle :

1. `deny 192.168.10.0 0.0.0.255` → bloque tout paquet venant du réseau 192.168.10.0/24
2. `permit any` → autorise tout le reste
3. Le masque **0.0.0.255** est un **wildcard mask** (inverse du masque de sous-réseau)

7. Wildcard Mask

Le wildcard mask indique quels bits de l'adresse IP doivent être vérifiés :

- **0** → le bit doit correspondre exactement
- **1** → le bit est ignoré (peu importe sa valeur)

Réseau	Masque	Wildcard
192.168.10.0/24	255.255.255.0	0.0.0.255
192.168.0.0/16	255.255.0.0	0.0.255.255
10.0.0.0/8	255.0.0.0	0.255.255.255
Hôte unique 192.168.10.5	—	0.0.0.0

Réseau	Masque	Wildcard
Tous (any)	—	255.255.255.255



`host 192.168.10.5` est équivalent à `192.168.10.5 0.0.0.0` `any` est équivalent à `0.0.0.0 255.255.255.255`

8. ACL Étendue — Exemple

Objectif : Autoriser le VLAN 10 à accéder uniquement au serveur web (HTTP/HTTPS) du VLAN 30, et bloquer tout autre accès au VLAN 30.

Placement : proche de la source → sur l'interface du routeur côté VLAN 10, en **in**.

```
ROUTEUR(config)# ip access-list extended ACCES-SERVEURS
ROUTEUR(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 host
192.168.30.10 eq 80
ROUTEUR(config-ext-nacl)# permit tcp 192.168.10.0 0.0.0.255 host
192.168.30.10 eq 443
ROUTEUR(config-ext-nacl)# deny   ip  192.168.10.0 0.0.0.255 192.168.30.0
0.0.0.255
ROUTEUR(config-ext-nacl)# permit ip  any any

ROUTEUR(config)# interface GigabitEthernet0/0.10
ROUTEUR(config-subif)# ip access-group ACCES-SERVEURS in
```

Lecture des règles :

1. Ligne 1 & 2 → autorise le TCP depuis VLAN 10 vers le serveur web sur les ports 80 et 443
2. Ligne 3 → bloque tout autre trafic IP depuis VLAN 10 vers VLAN 30
3. Ligne 4 → autorise tout le reste (autres VLANs non concernés par cette ACL)

Mots-clés pour les ports courants :

Mot-clé	Port	Protocole
eq 80	80	HTTP
eq 443	443	HTTPS
eq 22	22	SSH
eq 21	21	FTP
eq 53	53	DNS
eq 3389	3389	RDP

9. Cas Pratique : Protéger un VLAN Admin (Trafic de retour)

Objectif : Le VLAN 20 (IT / Admin) doit pouvoir accéder à tous les autres VLANs de l'entreprise, mais aucun autre VLAN ne doit pouvoir initier une connexion vers le VLAN IT.

Le piège du routeur “Stateless” : Contrairement à un pare-feu moderne, un routeur classique avec des ACL ne garde pas en mémoire l'état des connexions (il est “stateless”). Si l'administrateur lance un ping vers le VLAN USERS, le routeur laisse passer l'aller. Mais quand le PC USERS répond, le routeur voit cela comme un nouveau trafic. Si on bloque bêtement tout le trafic provenant de USERS vers IT, la réponse sera détruite et le ping échouera.

La solution : Il faut utiliser une ACL Étendue avec les arguments `established` (pour les sessions TCP déjà ouvertes par l'Admin) et `echo-reply` (pour les réponses aux pings de l'Admin).

Placement : Sur l'interface du VLAN IT (VLAN 20), en direction **out** (le trafic qui redescend du routeur vers les PC IT).

```
ROUTEUR(config)# ip access-list extended PROTECT-IT
! 1. Autoriser les réponses de ping (retour)
ROUTEUR(config-ext-nacl)# permit icmp any 192.168.20.0 0.0.0.255 echo-reply

! 2. Autoriser le trafic TCP de retour (navigation web, SSH, etc. initiés
par l'IT)
ROUTEUR(config-ext-nacl)# permit tcp any 192.168.20.0 0.0.0.255 established

! 3. Bloquer toute nouvelle requête provenant des autres VLANs (USERS et
SERVEURS)
ROUTEUR(config-ext-nacl)# deny ip 192.168.10.0 0.0.0.255 192.168.20.0
0.0.0.255
ROUTEUR(config-ext-nacl)# deny ip 192.168.30.0 0.0.0.255 192.168.20.0
0.0.0.255

! 4. Autoriser le reste du trafic au besoin
ROUTEUR(config-ext-nacl)# permit ip any any

ROUTEUR(config)# interface GigabitEthernet0/0.20
ROUTEUR(config-subif)# ip access-group PROTECT-IT out
```

10. Modifier une ACL nommée

Avec les ACL nommées, on peut supprimer une règle précise sans tout recréer :

```
! Afficher les règles avec leurs numéros de séquence
show access-lists ACCES-SERVEURS

! Supprimer une règle par son numéro de séquence
ROUTEUR(config)# ip access-list extended ACCES-SERVEURS
ROUTEUR(config-ext-nacl)# no 30          ! Supprime la règle numéro 30

! Insérer une règle à une position précise
ROUTEUR(config-ext-nacl)# 25 permit tcp 192.168.10.0 0.0.0.255 host
192.168.30.20 eq 22
```

11. Vérification

```
show access-lists                                ! Toutes les ACL avec
compteurs de hits
show access-lists ACCES-SERVEURS                 ! Une ACL spécifique
show ip interface GigabitEthernet0/0.10          ! ACL appliquées sur une
interface
clear ip access-list counters                    ! Remet les compteurs à zéro
```



Les **compteurs de hits** dans `show access-lists` indiquent combien de fois chaque règle a été déclenchée. C'est très utile pour déboguer : si le compteur d'une règle `permit` ne bouge pas, c'est qu'une règle `deny` plus haute intercepte le trafic avant.

12. Points clés à retenir

- Les règles sont lues **dans l'ordre** — l'ordre de saisie est important
- Tout ACL se termine par un **deny any implicite** — toujours finir par `permit any` si nécessaire
- ACL **standard** → près de la **destination**, filtre sur la source uniquement
- ACL **étendue** → près de la **source**, filtre sur src + dst + protocole + port
- Préférer les ACL **nommées** pour la lisibilité et la maintenabilité
- Une ACL ne peut être appliquée qu'**une seule fois par interface et par direction**

13. Imposer un chemin d’administration

Pour imposer un bastion, autoriser depuis celui-ci les protocoles nécessaires vers les serveurs cibles et vérifier le refus des accès directs depuis les autres zones. Une simple séparation en VLAN ne prouve pas que ces accès sont bloqués.

La recette doit comprendre un accès autorisé et un accès interdit, avec la source, la destination, le protocole et les compteurs de règles. Un ping seul ne valide pas le filtrage de SSH ou RDP.

Voir Guacamole et Diagnostic réseau.

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:cisco:cours:cours_acl

Last update: **2026/10/18 01:23**