**Documentation**

**Technique**

ligne horizontale

**Mise en place d’ACL pour DMZ et règles d’accès réseau interne**

ligne horizontale

# 

**25/04/2025**

**Gabriel PFISTER, Quentin PARC**

**Sommaire**

ligne horizontale

[**Contexte 3**](#_yqc3zntowln1)

[**Mise en place 3**](#_q0xtv7r3f5yl)

[ADMIN\_Access 3](#_fed8f9z44i70)

[ACL DMZ 4](#_u7f5t1acyevs)

# 

# Contexte



Une Access Control List (ACL) est un ensemble de règles définissant les permissions d’accès à des ressources informatiques. Ces règles spécifient quels systèmes ont le droit de communiquer avec une machine en fonction de leur adresse IP .Contexte et utilité des ACL

Les ACL sont utilisées dans divers domaines pour renforcer la sécurité des systèmes informatiques :

1. Sécurité du réseau
   * Elles permettent de contrôler l’accès au réseau en fonction des IP autorisé ou non.
2. Contrôle des accès réseau
   * Dans les pare-feu et routeurs, les ACL filtrent le trafic en autorisant ou bloquant certaines adresses IP, ports ou protocoles.
3. Sécurisation des systèmes d'exploitation
   * Les ACL sont utilisées pour restreindre l'accès aux applications et services système.

Afin de créer une DMZ autour de notre serveur Web public, il est utile de mettre en place des ACL, afin d'empêcher notre serveur Web de communiquer, tout en autorisant la connexion aux utilisateurs.

# Mise en place



Nous allons mettre en place plusieurs access-lists

La première que nous allons appeler ADMIN\_Access

## ADMIN\_Access

Autoriser uniquement les PC du VLAN 10 (administration) à se connecter aux serveurs via SSH (port 22) et Telnet (port 23).

Bloquer ces connexions pour tous les autres VLANs (ex. VLAN 20, 30...).

Laisser passer tout le reste du trafic (HTTP, ping, etc.).

En résumé :

Elle réserve l'accès aux connexions d'administration distante aux seuls administrateurs réseau

| # Création de l’ACL #  ip access-list extended Admin\_Access  # Autorise accès aux serveurs (ex : Telnet port 23, SSH port 22) # permit tcp 192.1.10.0 0.0.0.255 any eq 22 permit tcp 192.1.10.0 0.0.0.255 any eq 23 #Ici la communication n’est autorisé qu’avec le VLAN 10#  # Bloque les autres VLAN # deny tcp any any eq 22 deny tcp any any eq 23  # Autorise le reste # permit ip any any |
| --- |

## 

ACL DMZ  
Ensuite, nous allons créer une ACL spécifiquement pour créer une DMZ (autoriser les communication depuis les clients mais le serveur ne peux pas engagé de communication, il est obligé de répondre en fonction des requêtes)

Autoriser l'accès HTTP (port 80) au serveur Web public (en DMZ) depuis :

* Internet (WAN)
* Le réseau local (LAN : VLAN 10, 20, 30)

Autoriser les réponses des connexions déjà établies du serveur Web vers le LAN

Autoriser le ping (ICMP) pour les tests réseau

Bloquer tout autre trafic du serveur Web vers le LAN pour protéger le réseau interne

| # Création de l’ACL #  ip access-list extended DMZ\_FILTER  # Autoriser HTTP (port 80) vers le serveur Web depuis Internet #  permit tcp any host 10.29.231.150 eq 80  # Autoriser HTTP depuis le LAN (VLANs 10, 20, 30) # permit tcp 192.1.0.0 0.0.255.255 host 10.29.231.150 eq 80  # Autoriser les retours des connexions établies vers LAN (option 'established') # permit tcp host 10.29.231.150 192.1.0.0 0.0.255.255 established  # (facultatif) ICMP / ping autorisé pour tests # permit icmp any any echo permit icmp any any echo-reply  # Bloquer le reste (implicite ou explicite) # deny ip any 192.1.0.0 0.0.255.255 |
| --- |

## applique l’ACL sur int

## ACL\_Block\_Ping

Cette ACL permet comme son nom l’indique d'empêcher des pings depuis le serveur web vers membre du VLAN et autre

| ip access-list extended BLOCK\_PING\_DMZ # Bloquer ICMP (ping) du serveur Web vers le LAN # deny icmp host 10.29.231.150 192.1.0.0 0.0.255.255 echo deny icmp host 10.29.231.150 192.1.0.0 0.0.255.255 echo-reply  # Permettre tout le reste du trafic (autres services) # permit ip any any |
| --- |