








BTS SIO

# MISE EN PLACE DE RÈGLES ACL



HOUMADA Bilal

# PLAN DE LA SITUATION

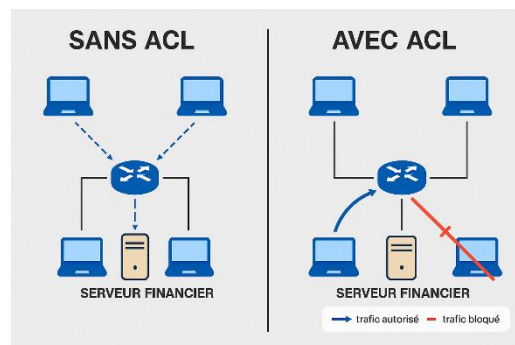
	Introduction.....
	Matériel et environnement utilisés.....
	Schéma Réseau Initial .....
	Objectifs des règles d'ACL.....
	Configuration des ACL.....
	Tests et Vérification.....
	Conclusion et Perspectives.....

# INTRODUCTION



Dans le cadre de ma formation BTS SIO – spécialité SISR au sein de l'établissement AURLOM, j'ai eu l'opportunité de réaliser un projet axé sur la mise en place de règles ACL (Access Control Lists).

Une ACL est une règle de filtrage appliquée sur un équipement réseau (généralement un routeur ou un commutateur) permettant de contrôler le trafic réseau en autorisant ou refusant certains flux en fonction de critères précis comme l'adresse IP source/destination, le protocole utilisé ou encore le port.



Ce projet a été réalisé dans un contexte de sécurisation d'un réseau interne, où il était nécessaire de limiter l'accès à certaines ressources selon les services ou les utilisateurs. Par exemple, seuls les postes du service comptabilité devaient

accéder au serveur financier, tandis que le reste du réseau devait en être isolé.

L'objectif était donc de définir et appliquer des règles ACL adaptées pour garantir la confidentialité et l'intégrité des échanges au sein du réseau.

# MATÉRIEL ET ENVIRONNEMENT UTILISÉS

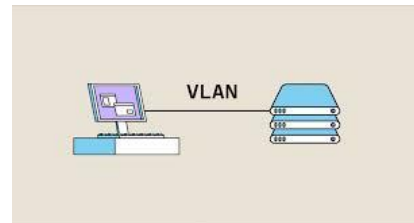
## ◆ **Routeur**

Dans ce projet, il permet aussi l'application des règles ACL pour filtrer le trafic.



## ◆ **Switchs avec VLANs**

Les commutateurs réseau (switchs) ont été configurés avec plusieurs VLANs (Virtual LANs) pour segmenter logiquement le réseau par services (ex : compta, RH, IT).



## ◆ **Machines clientes (PC simulés)**

Ordinateurs virtuels représentant les utilisateurs du réseau. Chaque PC appartient à un VLAN et teste l'accès aux ressources selon les règles ACL appliquées.

## ◆ Outils de test réseau

Utilisation de commandes comme :

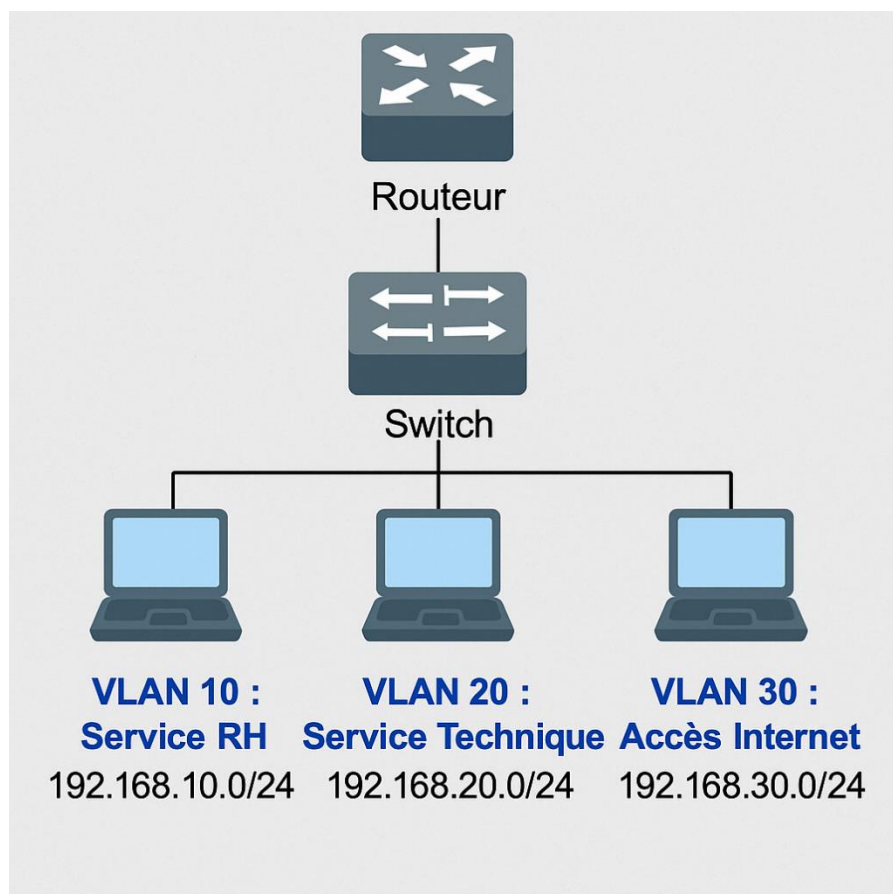
- Ping pour tester la **connectivité**
- traceroute pour analyser le **chemin réseau**

# SCHÉMA RÉSEAU INITIAL

Le réseau est composé de 3 VLANs :

- VLAN 10 : Service RH (192.168.10.0/24)
- VLAN 20 : Service Technique (192.168.20.0/24)
- VLAN 30 : Accès Internet (192.168.30.0/24)

Tous les VLANs sont reliés à un routeur permettant le routage inter-VLAN.

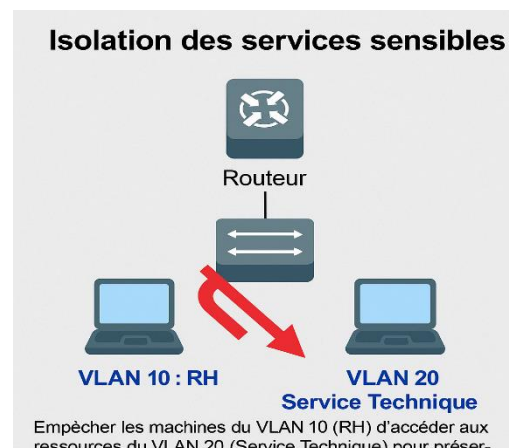


# OBJECTIFS DES RÈGLES ACL

L'objectif principal de la mise en place des règles ACL est de renforcer la sécurité et le contrôle du trafic réseau en filtrant les communications entre les différents VLANs. Voici les règles appliquées dans ce projet :

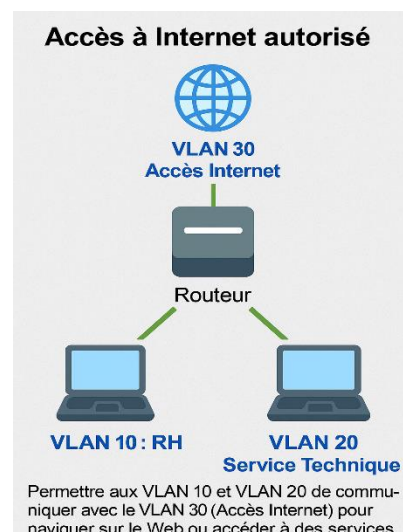
## ◆ 1. Isolation des services sensibles

🔒 Empêcher les machines du VLAN 10 (RH) d'accéder aux ressources du VLAN 20 (Service Technique) pour préserver la confidentialité des données techniques.



## ◆ 2. Accès à Internet autorisé

🌐 Permettre aux VLAN 10 et VLAN 20 de communiquer avec le VLAN 30 (Accès Internet) pour naviguer sur le Web ou accéder à des services en ligne.



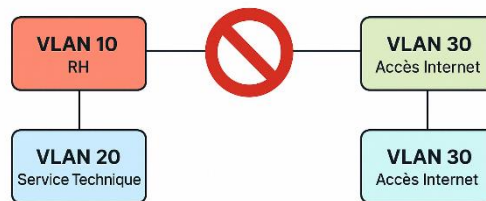


### ◆ 3. Blocage par défaut des autres communications

🚫 Bloquer tout accès non autorisé entre les VLANs, sauf les exceptions définies. Cela limite les risques de propagation de menaces internes et cloisonne les services.

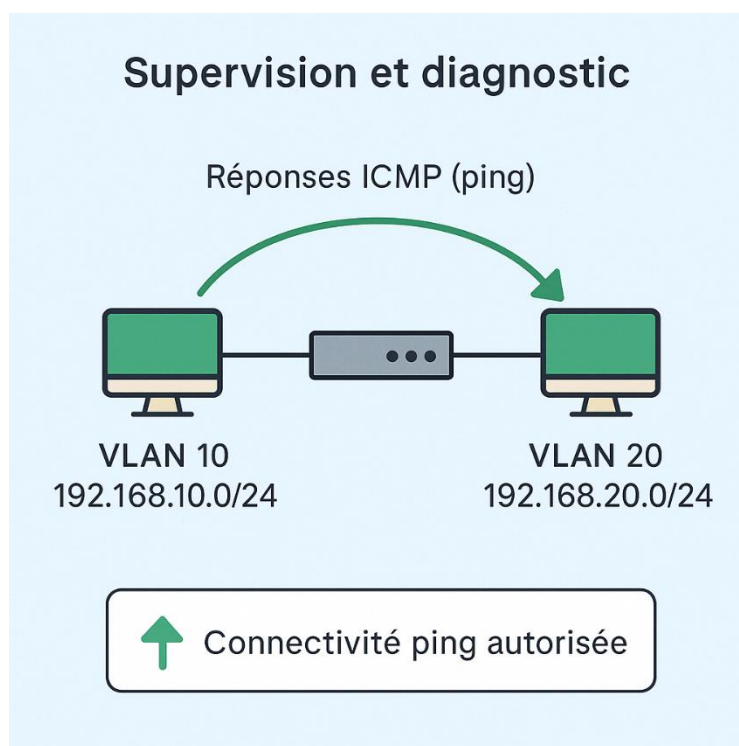
- 3. Blocage par défaut des autres communications

🚫 Bloquer tout accès non autorisé entre les VLANs, sauf les exceptions définies. Cela limite les risques de propagation de menaces internes et cloisonne les services.



### ◆ 4. Supervision et diagnostic

🔍 Autoriser les réponses ICMP (ping) entre les postes clients internes pour assurer un minimum de connectivité nécessaire à la supervision réseau et au diagnostic des problèmes.



# CONFIGURATION DES ACL

Des **ACL étendues** ont été créées sur le **routeur** afin de filtrer les communications entre les différents VLANs. Ces listes de contrôle d'accès ont été **appliquées en entrée** sur les interfaces VLAN concernées.

! ACL pour VLAN 10 : peut accéder à VLAN 20 et 30 (Internet)

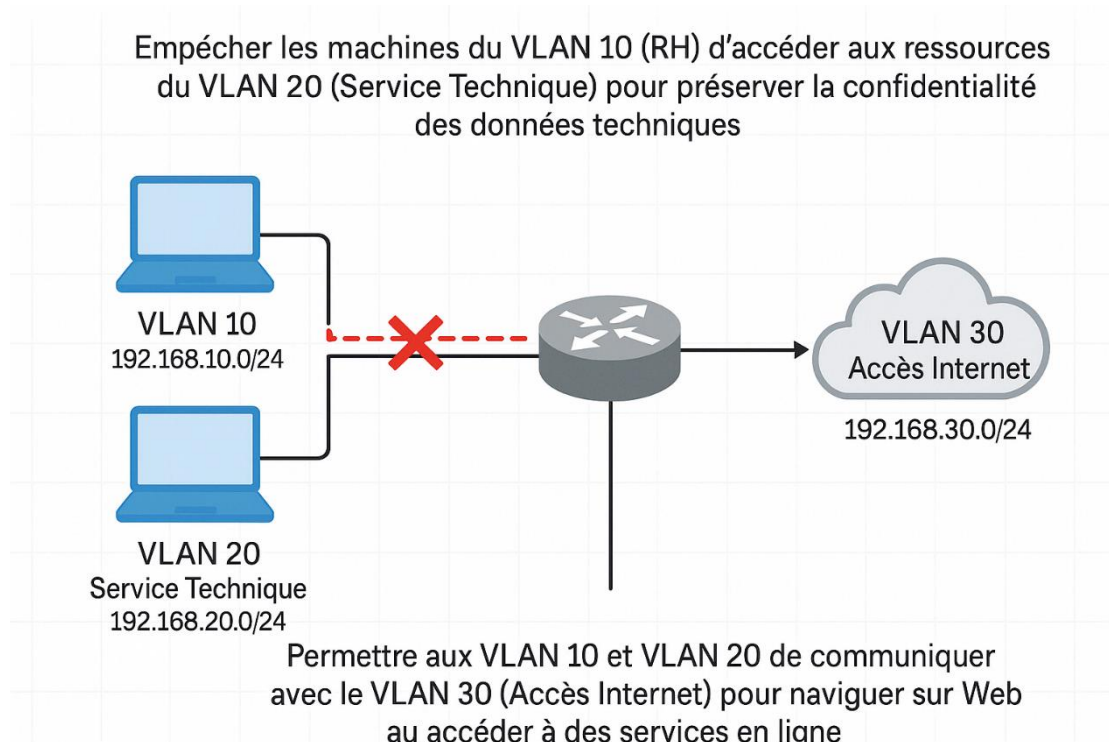
```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 101 deny ip 192.168.10.0 0.0.0.255 any
access-list 101 permit ip any any
```

! ACL pour VLAN 20 : peut accéder à VLAN 30 uniquement

```
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 102 deny ip 192.168.20.0 0.0.0.255 any
access-list 102 permit ip any any
```

! ACL pour VLAN 30 : accès Internet uniquement (aucun retour vers VLAN 10/20)

```
access-list 103 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 103 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 103 permit ip any any
```



## ACL pour VLAN 10

```
Access List 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

→ Autorise aussi l'accès du VLAN 10 au **VLAN 30 (Internet)**.

```
Access List 101 deny ip 192.168.10.0 0.0.0.255 any
```

→ **Bloque tout autre trafic sortant** du VLAN 10 vers d'autres VLANs ou destinations.

```
access-list 101 permit ip any any
```

→ Cette ligne est une **sécurité pour éviter un blocage total**, elle permet **tout autre trafic entrant** non concerné (en général, retour de communication autorisée).

## ACL pour VLAN 20

```
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
```

→ Permet au VLAN 20 d'accéder au **VLAN 30 (Internet)**.

```
access-list 102 deny ip 192.168.20.0 0.0.0.255 any
```

→ **Bloque tout autre trafic** depuis le VLAN 20.

```
access-list 102 permit ip any any
```

→ Même logique que pour VLAN 10, pour ne pas bloquer d'autres communications système (ex : réponse ping autorisée, supervision...).

## ACL pour VLAN 30 (Internet)

```
access-list 103 deny ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
```

```
access-list 103 deny ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
```

→ **Interdit tout retour de trafic** du VLAN 30 (Internet) vers les VLAN internes (10 et 20) pour éviter les attaques entrantes.

```
access-list 103 permit ip any any
```

→ Autorise tout le reste (ex : réponse DNS, retour HTTP autorisé si initié par un poste interne).

# TESTS ET VÉRIFICATIONS

Des tests ont été réalisés pour **valider le bon fonctionnement des règles ACL** à l'aide de commandes **ping** et **tests d'accès HTTP** (navigateur ou curl) :

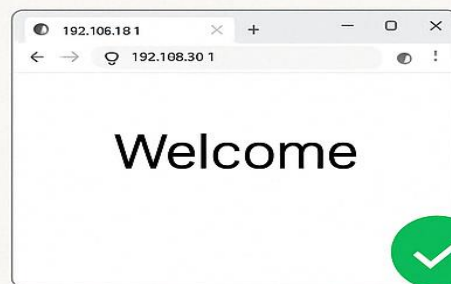
## TESTS ET VÉRIFICATIONS

VLAN 10 → VLAN 20 :  
accès refusé

```
C:>ping 192.168.20.2
Pinging 192.168.20.2 with 32 bytes of data:
Request timed out.
Request timed out.
4 Packets loss
Distribution: 4 = 100%
```



VLAN 10 → Internet:  
accès autorisé



VLAN 20 → VLAN 10 :  
accès autorisé (par défaut)

```
C:>ping 192.168.10.2
Pinging 192.168.10.2 with 32 bytes of data:
Request timed out.
Request timed out.
4 Packets loss
Distribution: 4 = 100%
```



Ping inter-VLAN ; autorisé  
si non filtré par ACL ICMP

```
C:>ping 192.168.20.2
Pinging 192.168.20.2 with 32 bytes of data:
Request timed out.
Request timed out.
4 Packets loss
Distribution: 4 = 100%
```



# CONCLUSION ET PERSPECTIVES

Ce projet m'a permis de renforcer mes compétences en configuration réseau et en sécurisation des flux. J'ai appris à créer des ACL précises, adaptées à des besoins spécifiques, à les tester rigoureusement et à ajuster les règles en cas de comportement inattendu.

Cette mise en œuvre m'a également sensibilisé à l'importance de la segmentation réseau et du contrôle d'accès dans un environnement professionnel.

