# Mise en place d'ACL Étendues chez GTECH

Tableau de matières

# Cahier des charges - Mise en place d'ACL Étendues chez GTECH

## 1. Contexte et Problématiques

### Contexte actuel

L'entreprise GTECH dispose d'une infrastructure réseau composée de deux réseaux locaux (LAN) interconnectés via une liaison WAN entre deux routeurs Cisco. Le premier réseau héberge les postes utilisateurs (dont le poste d'administration PC0) et le second héberge les serveurs Web de l'entreprise. À ce jour, le routage assure une connectivité totale entre tous les équipements sans aucune restriction.

### Problématique identifiée

L'absence de filtrage entre le réseau utilisateur et le réseau serveur pose un problème majeur de sécurité. Actuellement, n'importe quel utilisateur peut accéder à l'ensemble des services (Web et ICMP) des serveurs, ce qui expose l'entreprise à des risques de mauvaises manipulations, d'intrusions internes ou de saturation réseau inutile. Il est impératif de segmenter les flux pour ne laisser passer que le strict nécessaire.

## 2. Expression des besoins

### Besoins fonctionnels

GTECH a défini une politique de sécurité précise qui doit être implémentée techniquement :

- **Règle 1 (Accès Web A) :** Le poste d'administration (PC0 - 192.168.1.2) **doit pouvoir accéder** au site web du Serveur A (192.168.2.2) via le protocole HTTP (port 80).
- **Règle 2 (Restriction Web B) :** Le poste PC0 **ne doit pas pouvoir accéder** au site web du Serveur B (192.168.2.3) en HTTP.
- **Règle 3 (Maintenance Serveur B) :** Le poste PC0 **doit pouvoir tester la connectivité** (Ping/ICMP) vers le Serveur Web B.
- **Règle 4 (Restriction Serveur A) :** Le poste PC0 **ne doit pas pouvoir pinger** le Serveur Web A (sécurité par obscurité sur le protocole ICMP).

## 3. Description de l'existant

L'infrastructure technique en place sur laquelle le projet doit se greffer est la suivante :

- **Architecture :** 2 sites reliés par une liaison série/WAN (10.0.0.0/30).
- **Matériel Réseau :**
  - 2 Routeurs Cisco (modèle 1841).
  - 2 Commutateurs Cisco (modèles 2960/2950).
- **Adressage IP :**
  - Réseau Clients : 192.168.1.0/24 (Passerelle : 192.168.1.1).
  - Réseau Serveurs : 192.168.2.0/24 (Passerelle : 192.168.2.1).

### Détail des Services Web (Configuration actuelle)

Les serveurs sont pré-configurés avec les paramètres suivants pour simuler les applications métiers :

- **Serveur Web A**
  - IP : 192.168.2.2 / Masque : 255.255.255.0 / Passerelle : 192.168.2.1
  - **Contenu Page Web :** "Bienvenue sur le serveur Web A"
- **Serveur Web B**
  - IP : 192.168.2.3 / Masque : 255.255.255.0 / Passerelle : 192.168.2.1
  - **Contenu Page Web :** "Bienvenue sur le serveur Web B"

# 4. Analyse des choix techniques

Pour répondre aux besoins de filtrage sélectif, nous avons analysé les méthodes disponibles sur le matériel Cisco existant.

### Comparaison des méthodes

- **Option A : ACL Standard**
  - *Fonctionnement :* Filtre uniquement sur l'adresse IP source.
  - *Verdict :* **Rejetée**. Elle ne permet pas de différencier le trafic Web (port 80) du trafic Ping (ICMP). Si on bloque l'un, on bloque l'autre pour une même destination.
- **Option B : ACL Étendue**
  - *Fonctionnement :* Filtre selon l'IP source, l'IP destination, le protocole (TCP/UDP/ICMP) et le port.
  - *Verdict :* **Retenue**. C'est la seule solution technique native permettant d'autoriser le Ping tout en bloquant le Web (et inversement) vers des cibles spécifiques.

### Le projet retenu

La solution consistera à déployer une **ACL Étendue (numéro 100)** sur le **Routeur Gauche** (côté utilisateur). L'ACL sera appliquée en **entrée (in)** sur l'interface FastEthernet0/1 pour filtrer les paquets dès leur arrivée sur le routeur, optimisant ainsi les ressources de la bande passante WAN.

# 5. Étude comparative d'outils du marché et décision finale

Une veille rapide a permis de comparer la solution retenue face à une alternative matérielle.

| Solution | Fournisseur | Coût | Avantages | Inconvénients |
|---|---|---|---|---|
| **ACL sur Routeur (IOS)** | Cisco (Existant) | **0 € (Inclus)** | Rapide, pas de nouveau matériel, très granulaire. | Gestion en ligne de commande (CLI). |
| **Pare-feu dédié (ASA)** | Cisco / Fortinet | Élevé (> 500€) | Interface graphique, inspection profonde (DPI). | Surcoût inutile pour un besoin de filtrage simple. |

Décision finale :
Le projet sera réalisé en utilisant les fonctionnalités ACL Étendues intégrées aux routeurs actuels, garantissant un coût nul en matériel et une réponse parfaite au cahier des charges.

# 6. Prix de l'intervention

Voici le devis estimatif pour la réalisation de ce projet de sécurisation :

| Poste de dépense | Durée estimée | Tarif horaire | Total HT |
|---|---|---|---|
| Analyse de l'architecture et plan d'adressage | 2 heures | 70 € | 140 € |
| Configuration du routage et des interfaces | 3 heures | 70 € | 210 € |
| Écriture et déploiement des règles ACL | 2 heures | 70 € | 140 € |
| Tests de validation | 1 heure | 70 € | 70 € |

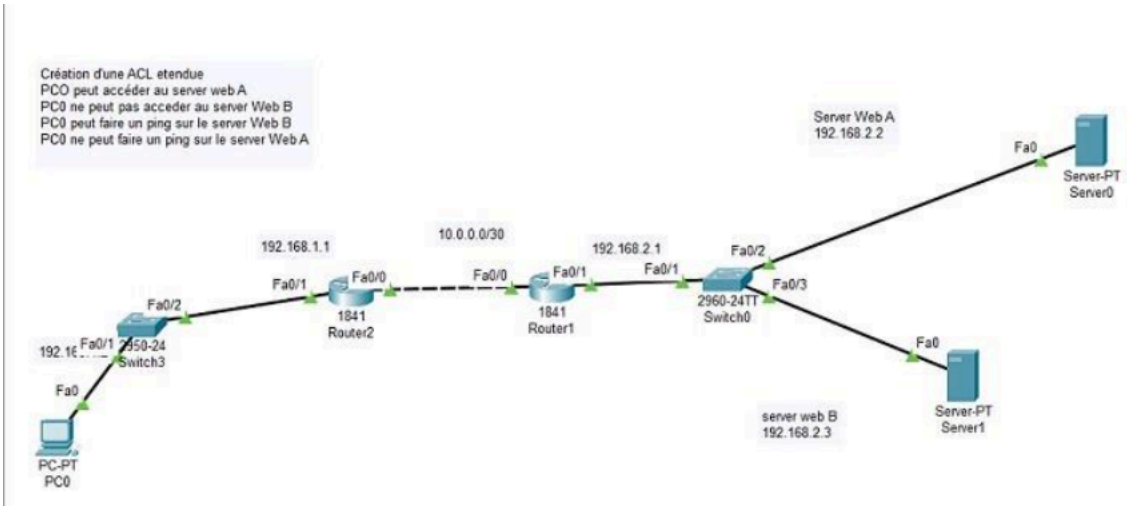
| | | | |
|---|---|---|---|
| (Ping & HTTP) et Recette | | | |
| **TOTAL PROJET** | **8 heures** | | **560 €** |

# 7. Schéma du projet et Mise en œuvre

Cette section présente l'architecture déployée et les preuves de fonctionnement.

## A. Topologie Réseau

Voici le schéma de l'infrastructure simulée sous Packet Tracer, montrant les deux zones (Utilisateurs et Serveurs) et les routeurs interconnectés.




Ce schéma permet de visualiser où l'ACL est placée (Routeur de gauche).

## B. Configuration Technique (Commandes)

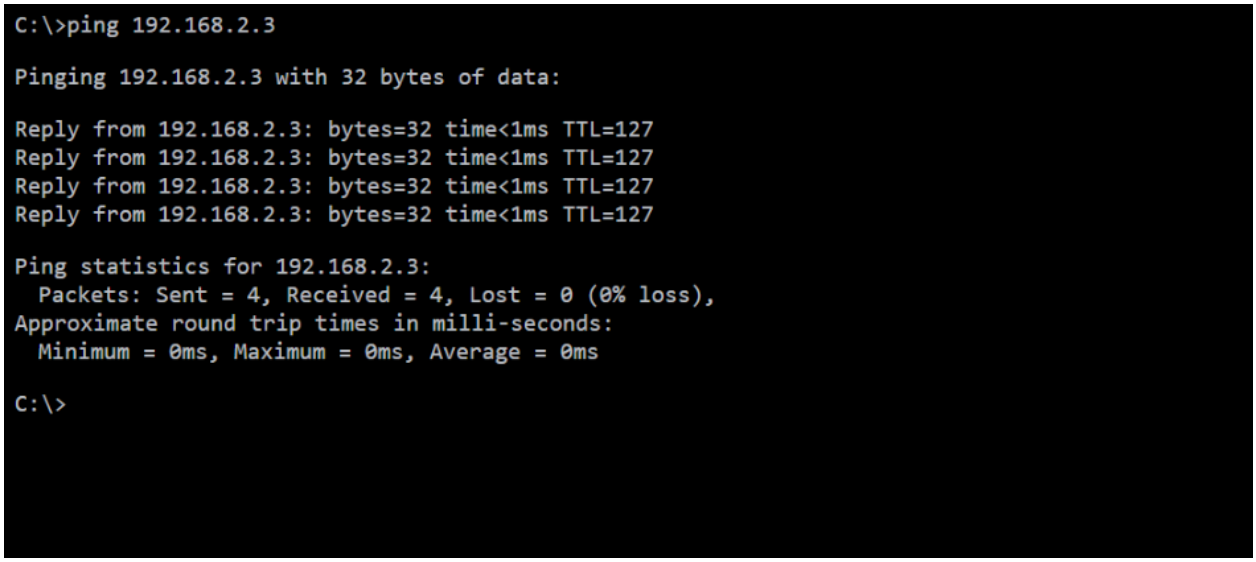
Les commandes suivantes ont été injectées dans le routeur pour activer la sécurité :

Router(config)# access-list 100 permit tcp host 192.168.1.2 host 192.168.2.2 eq 80
Router(config)# access-list 100 deny tcp host 192.168.1.2 host 192.168.2.3 eq 80
Router(config)# interface fa0/1
Router(config-if)# ip access-group 100 in

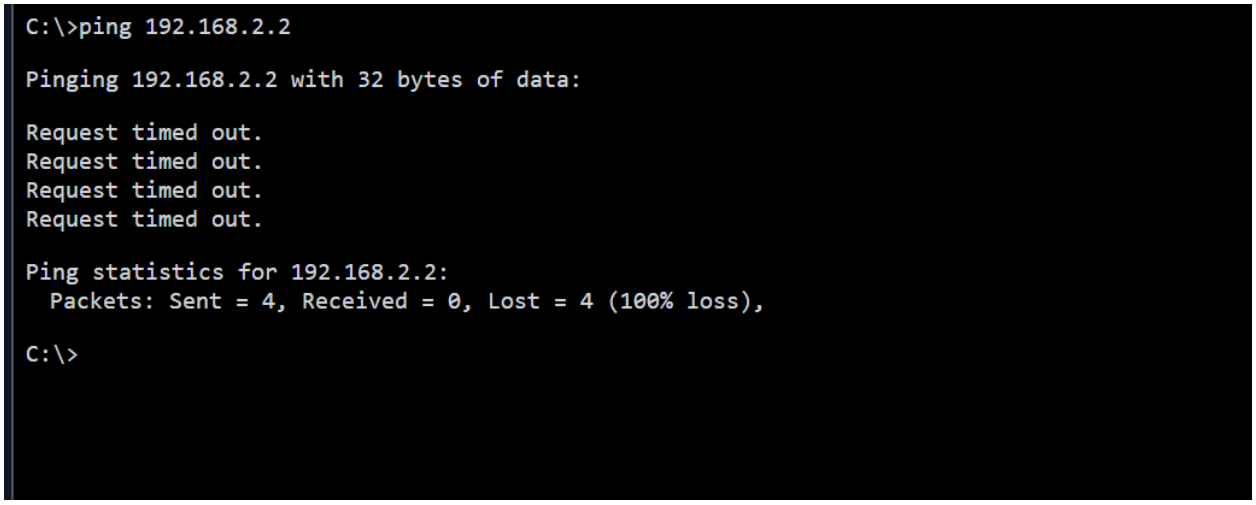
## C. Preuves de fonctionnement (Screens)

1. Validation des règles ICMP (Ping)
Le test ci-dessous montre que le Ping fonctionne vers le Serveur B (autorisé) mais échoue

vers le Serveur A (interdit).




*ping réussie vers le server B*




*Ping échoué vers le server Web A*

2. Validation des règles HTTP (Web)
Le test ci-dessous montre l'accès réussi au site A ("Bienvenue sur le serveur Web A") et le blocage de l'accès au site B.

*Bienvenue sur le Server Web A*

*Request Timeout*

## 8. Conclusion

La mise en place de l'ACL étendue a été réalisée avec succès. Nous avons configuré le routeur pour filtrer précisément le trafic entre le réseau utilisateur et le réseau serveur. Les tests ont confirmé que les accès Web et Ping sont désormais strictement contrôlés selon la politique de sécurité de GTECH, assurant ainsi la protection des données et des services de l'entreprise.