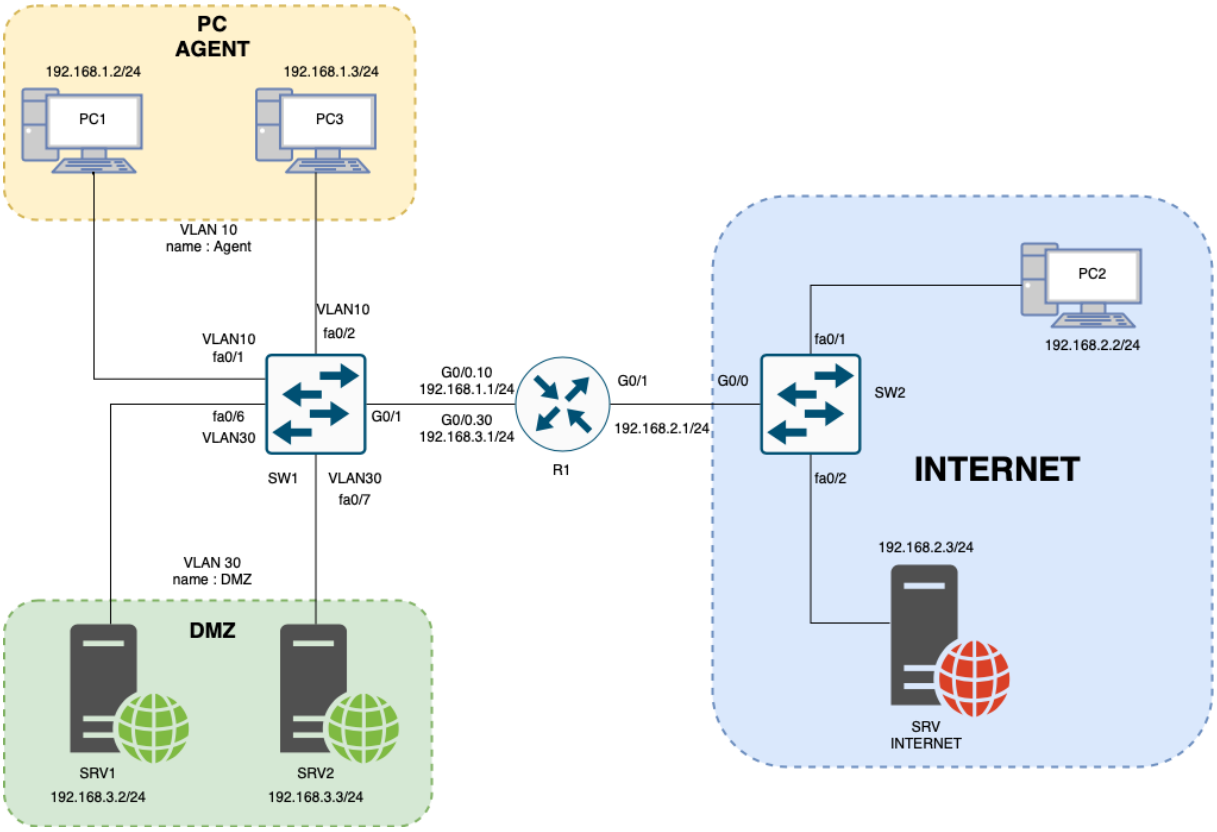
CRÉATION D'UNE DMZ À L'AIDE DES LISTES DE CONTRÔLE D'ACCÈS (ACL)



Objectif terminal :

Dans le domaine de la sécurité des réseaux, les **listes de contrôle d'accès (ACL)** jouent un rôle essentiel pour filtrer le trafic et limiter l'accès aux ressources critiques. Elles permettent d'autoriser ou de bloquer des communications en fonction d'un ensemble de règles définies par l'administrateur réseau.

L'objectif de ce TP est d'apprendre à configurer progressivement des **ACL standard et étendues** afin de sécuriser un réseau et d'implémenter une **DMZ (zone démilitarisée)**, un élément clé pour isoler les services accessibles depuis l'extérieur.

Nous commencerons par la mise en place d'une **topologie simple** autour d'un **routeur**, où nous apprendrons à configurer des **ACL standard** pour contrôler le trafic basé uniquement sur les adresses IP sources. Ensuite, nous **complexifierons progressivement l'architecture** en introduisant des **ACL étendues**, qui permettent un filtrage plus précis basé sur plusieurs critères, tels que l'adresse source, l'adresse destination, les ports et les protocoles.
Enfin, nous appliquerons ces connaissances à la configuration d'une **infrastructure intégrant une DMZ**, où nous définirons des règles de filtrage permettant de contrôler **l'accès aux services publics** tout en **protégeant le réseau interne** contre les menaces externes.

À travers ce TP, vous développerez des compétences essentielles pour **concevoir et sécuriser une architecture réseau**, tout en maîtrisant l'utilisation des **ACL sur un routeur** pour la mise en place d'une **politique de sécurité efficace**.

1. Introduction aux listes de contrôle d'accès standard :

Les **listes de contrôle d'accès (ACL) standard** sont un mécanisme de filtrage utilisé sur les routeurs pour **restreindre le trafic réseau** en fonction de **l'adresse IP source**. Elles permettent **d'autoriser ou de bloquer** des paquets **sans prendre en compte l'adresse de destination, les ports ou les protocoles**.

Les ACL standard utilisent des **numéros compris entre 1 et 99**, ainsi que **1300-1999** pour les versions étendues de cette plage. Elles sont généralement appliquées sur une interface en entrée (**inbound**) ou en sortie (**outbound**) afin de **limiter l'accès aux ressources réseau**.

Les ACL sont évaluées **de haut en bas**, règle par règle, dans l'ordre où elles ont été configurées. Dès qu'un paquet correspond à une règle, **celle-ci est appliquée et les règles suivantes ne sont pas analysées**. Si aucune correspondance n'est trouvée, une règle implicite **"deny all"** bloque le trafic par défaut. Il est donc essentiel d'organiser les règles de manière stratégique : les plus spécifiques doivent être placées en premier pour éviter qu'une règle trop large ne bloque ou autorise du trafic indésirable.

Syntaxe de base :

```
access-list [numéro] {permit|deny} [adresse_source] [wildcard]
```

Exemple pour bloquer l'accès à une adresse IP spécifique :

```
access-list 10 deny 192.168.1.10 0.0.0.0
access-list 10 permit 192.168.1.0 0.0.0.255
```

Puis, application sur une interface :

```
interface GigabitEthernet0/0
ip access-group 10 in
```

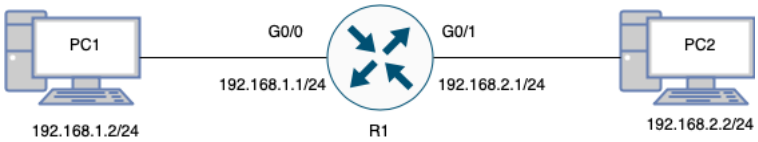
Dans cet exemple, un paquet provenant de **192.168.1.10** sera bloqué immédiatement par la première règle, tandis qu'un paquet venant de **192.168.1.25** sera autorisé par la seconde. En revanche, un paquet venant de **10.0.0.5** sera bloqué, car il ne correspond à aucune règle explicite et sera donc rejeté par la règle implicite "deny all".

Bonnes pratiques :

- **Placer les ACL standard aussi près que possible de la destination** pour éviter un filtrage trop large.
- Toujours **ajouter une règle "permit any"** à la fin si l'on ne veut pas bloquer tout le trafic.
- **Optimiser l'ordre des règles** en plaçant les règles spécifiques avant les règles générales.
- Ne pas oublier que **par défaut, tout ce qui n'est pas explicitement autorisé est bloqué**.

Les ACL standard sont simples mais limitées, car elles ne tiennent compte que de l'adresse source. Pour un filtrage plus précis (basé sur la destination, le protocole ou les ports), on utilisera les **ACL étendues**.

Topologie 1 :



📌 Objectif :
Utiliser les access-lists standard pour bloquer les pings provenant du PC 192.168.1.2/24.

Questions :

1. **Saisissez** le schéma de la topologie sur packet tracer.
2. **Configurez** les interfaces du routeur et les adresses IP des PC.
3. **Proposez** une access-list pour bloquer les pings provenant du PC 192.168.1.1.
4. **Configurez** le routeur avec la proposition précédente.
5. **Testez** votre configuration pour un ping de PC1 vers PC2.
6. **Testez** votre configuration pour un ping de PC2 vers PC1. Que constatez-vous ?

2. Introduction aux listes de contrôle d'accès étendues :

Les listes de contrôle d'accès (ACL) étendues offrent un filtrage plus précis du trafic réseau en permettant de spécifier plusieurs critères : l'adresse IP source et destination, le protocole (TCP, UDP, ICMP, etc.), ainsi que les ports concernés. Elles permettent ainsi de contrôler finement le trafic et de mettre en place des règles de sécurité avancées.

Les ACL étendues utilisent des numéros compris entre 100 et 199, ainsi que 2000-2699 pour les versions numérotées étendues. Contrairement aux ACL standard, qui filtrent uniquement en fonction de l'adresse source, les ACL étendues permettent de restreindre l'accès à des services spécifiques ou d'empêcher certains types de connexions entre différentes parties du réseau.

Comme les ACL standard, elles sont évaluées de haut en bas, dans l'ordre où elles ont été définies. Dès qu'une règle correspond au paquet, elle est appliquée et les règles suivantes ne sont plus prises en compte. Si aucune règle ne correspond, le paquet est bloqué par défaut à cause de la règle implicite "deny all". Il est donc crucial de bien organiser les règles, en plaçant les plus spécifiques en premier pour éviter des filtrages involontaires.

Syntaxe de base :

```
access-list [numéro] {permit|deny} [protocole] [adresse_source]
[wildcard] [opérateur_port] [adresse_destination] [wildcard]
[opérateur_port]
```

Exemple pour autoriser uniquement l'accès SSH (port 22) depuis un réseau spécifique :

```
access-list 110 permit tcp 192.168.1.0 0.0.0.255 any eq 22
access-list 110 deny ip any any
```

Puis, application sur une interface :

```
interface GigabitEthernet0/1
ip access-group 110 in
```

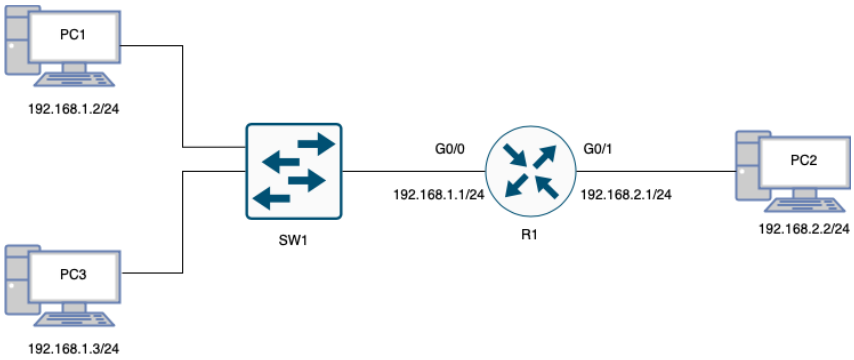
Dans cet exemple, seul le trafic SSH provenant du réseau 192.168.1.0/24 sera autorisé, tandis que tout le reste sera bloqué.

Bonnes pratiques :

- Placer les ACL étendues aussi près que possible de la source pour éviter que du trafic indésirable traverse le réseau inutilement.
- Optimiser l'ordre des règles en plaçant les plus précises avant les règles plus générales.
- Utiliser des commentaires (remark) pour documenter les règles et faciliter leur compréhension.
- Ne pas oublier la règle implicite "deny all", qui bloque tout le trafic non explicitement autorisé.

Grâce à leur flexibilité, les ACL étendues sont particulièrement adaptées pour protéger des services sensibles, segmenter un réseau et sécuriser une DMZ.

Topologie 2 :



📌 Objectif :

Configurer une ACL étendue afin de contrôler les communications ICMP (ping) entre trois machines : PC1 (192.168.1.2/24), PC2 (192.168.2.2/24) et PC3 (192.168.1.3/24).

🔷 Règles de filtrage à appliquer :

1. Bloquer les pings de PC2 (192.168.2.2) vers PC1 (192.168.1.2).
2. Autoriser uniquement les pings de PC2 vers PC3 (192.168.1.3).
3. Ne pas restreindre les pings émis par PC1 :
    - PC1 doit pouvoir envoyer des pings vers PC2 et PC3.
4. Ne pas restreindre les pings émis par PC3 :
    - PC3 doit pouvoir envoyer des pings vers PC1 et PC2.

Ces règles garantissent que PC2 ne peut pinguer que PC3, tout en laissant les autres communications ICMP libres.

🔥 Effet attendu :

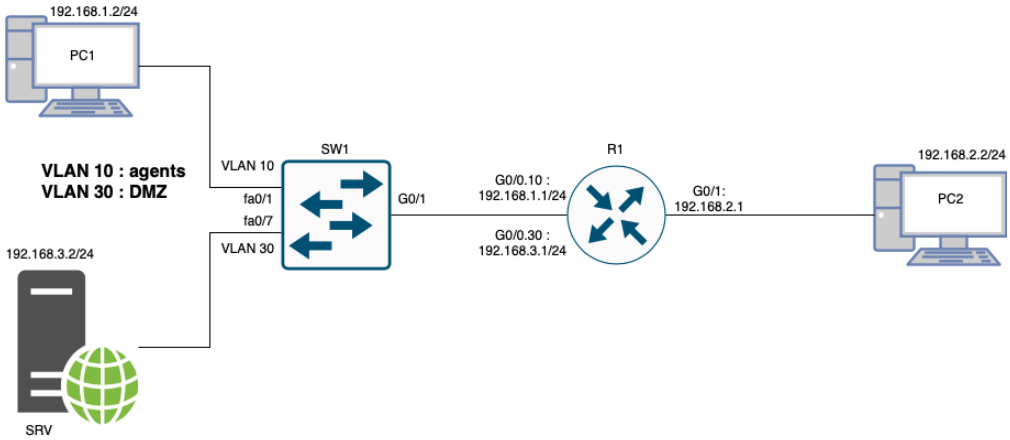
✔ PC1 peut envoyer des pings vers PC2 et PC3 sans restriction.
✔ PC3 peut envoyer des pings vers PC1 et PC2 sans restriction.
✔ PC2 peut envoyer des pings vers PC3.

❌ PC2 ne peut pas envoyer de pings vers PC1.
✔ Toutes les autres communications ICMP non spécifiées restent libres.
👉 Cette configuration garantit que PC2 est limité dans ses communications ICMP, alors que PC1 et PC3 ont un accès total aux pings.

Questions :

1. **Saisissez** le schéma de la topologie 2.
2. **Configurez** les interfaces du routeur et les adresses IP des PC.
3. **Proposez** une acces-list permettant la réalisation de l'objectif décrit ci-dessus.
4. **Configurez** le routeur avec la proposition précédente.
5. **Testez** votre configuration pour un ping de PC1 vers PC2.
6. **Testez** votre configuration pour un ping de PC2 vers PC1.
7. **Testez** votre configuration pour un ping de PC2 vers PC3.
8. **Testez** votre configuration pour un ping de PC3 vers PC2.
9. **Testez** votre configuration pour un ping de PC1 vers PC3.
10. **Testez** votre configuration pour un ping de PC3 vers PC1.

Topologie 3 :



📌 Objectif :
Configurer une ACL étendue afin de contrôler le trafic ICMP (ping) entre deux VLANs et un réseau extérieur :

- VLAN 10 - Agents (192.168.1.0/24)
- VLAN 30 - DMZ (192.168.3.0/24)
- Réseau extérieur (192.168.2.0/24)

🔷 Règles à appliquer :

1. Bloquer les pings du réseau extérieur (192.168.2.0/24) vers le VLAN 10 (192.168.1.0/24).
2. Autoriser uniquement les pings du réseau extérieur vers le VLAN 30 (192.168.3.0/24).
3. Autoriser les pings émis depuis le VLAN 10 et le VLAN 30 vers le réseau extérieur.
4. Empêcher le VLAN 30 (192.168.3.0/24) d'accéder au VLAN 10 (192.168.1.0/24).

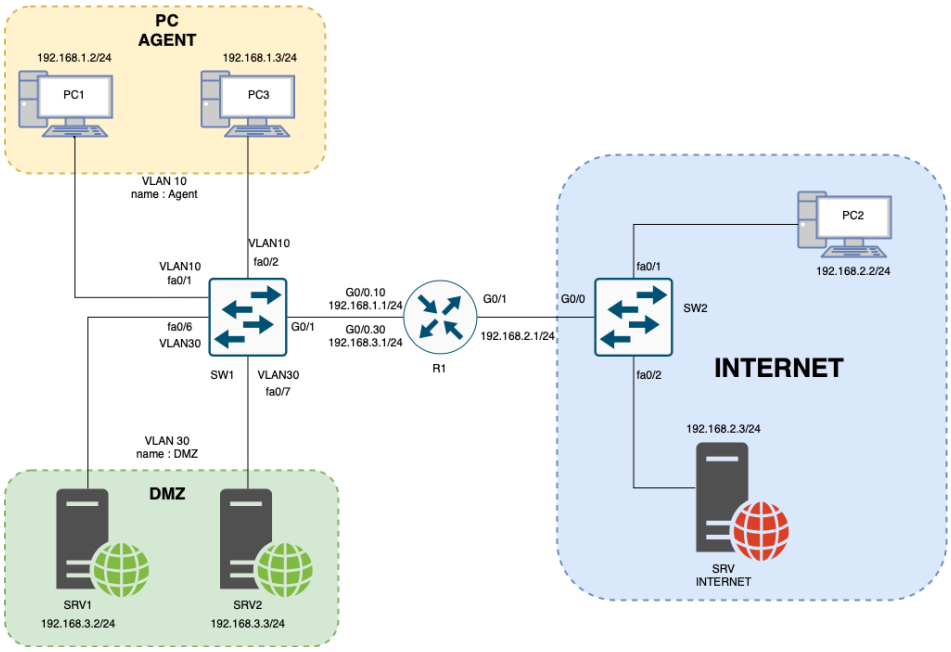
🔥 Effet attendu :
✔ Le réseau extérieur peut pinguer uniquement le VLAN 30 (DMZ).
✔ Le VLAN 10 et le VLAN 30 peuvent pinguer vers l'extérieur sans restriction.

❌ Le réseau extérieur ne peut pas pinguer le VLAN 10 (Agents).
❌ Le VLAN 30 (DMZ) ne peut pas communiquer avec le VLAN 10 (Agents).

Questions :

1. **Saisissez** le schéma de la topologie 3.
2. **Configurez** les adresses IP des PC.
3. **Créez** les VLANs sur le switch.
4. **Associez** les interfaces aux VLANs sur le switch.
5. **Configurez** le routage inter-vlan sur le routeur.
6. **Testez** les connexions entre les différents PC.
7. **Proposez** une access-list pour réaliser la liaison réseau extérieur-VLAN 10.
8. **Configurez** le routeur avec la proposition précédente.
9. **Testez** votre configuration pour un ping de PC1 vers PC2.
10. **Testez** votre configuration pour un ping de PC2 vers PC1.
11. **Proposez** une access-list pour réaliser la liaison VLAN30-VLAN 10.
12. **Configurez** le routeur avec la proposition précédente.
13. **Testez** votre configuration pour un ping de SRV vers PC1.
14. **Testez** votre configuration pour un ping de PC1 vers SRV.
15. **Testez** votre configuration pour un ping de SRV vers PC2.
16. **Testez** votre configuration pour un ping de PC2 vers SRV.

Topologie 4 :



📌 Objectif :
Configurer une ACL étendue afin de contrôler l'accès entre deux réseaux VLANs et un réseau extérieur, en sécurisant les communications tout en permettant l'accès aux services nécessaires.

Topologie :

- VLAN Agents (192.168.1.0/24) : Contient PC1 et PC3.
- VLAN DMZ (192.168.3.0/24) : Contient SRV1 et SRV2 (serveurs web internes).
- Réseau extérieur (192.168.2.0/24) : Contient PC2 et SRV Internet (serveur web accessible depuis l'extérieur).

🔷 Règles de filtrage à appliquer :

1. Interdire l'accès au VLAN Agents (192.168.1.0/24) depuis l'extérieur (192.168.2.0/24).
2. Autoriser uniquement l'accès au VLAN DMZ (192.168.3.0/24) depuis l'extérieur (192.168.2.0/24).
3. Interdire l'accès au VLAN Agents (192.168.1.0/24) depuis le VLAN DMZ (192.168.3.0/24).
4. Autoriser les pings du VLAN Agents vers le VLAN DMZ.
5. Autoriser l'accès aux serveurs web du VLAN DMZ (SRV1 et SRV2) depuis le VLAN Agents (192.168.1.0/24).
6. Autoriser l'accès au serveur web Internet (SRV Internet) situé sur le réseau extérieur (192.168.2.0/24) depuis les VLAN Agents et DMZ.

🔥 Effet attendu :

✔ Depuis l'extérieur (192.168.2.0/24), seuls les serveurs du VLAN DMZ (Srv1 et Srv2) sont accessibles.

❌ Depuis l'extérieur, il est impossible d'accéder au VLAN Agents (192.168.1.0/24).

❌ Depuis le VLAN DMZ, l'accès au VLAN Agents est interdit.

✔ Depuis le VLAN Agents (PC1 et PC3), il est possible de pinguer les serveurs du VLAN DMZ.

✔ Depuis le VLAN Agents, l'accès aux serveurs web du VLAN DMZ (Srv1 et Srv2) est autorisé.

✔ Depuis le VLAN Agents et le VLAN DMZ, l'accès au serveur web Internet (SRV Internet) est autorisé.

👉 Cette configuration garantit une segmentation réseau sécurisée où seuls les accès nécessaires sont autorisés, tout en maintenant l'accès aux services web internes et externes.

Questions :

1. **Saisissez** le schéma de la topologie 4.
2. **Configurez** les adresses IP des PC.
3. **Créez** les VLANs sur le switch.
4. **Associez** les interfaces aux VLANs sur le switch.
5. **Configurez** le routage inter-vlan sur le routeur.
6. **Testez** les connexions entre les différents PC et serveur.
7. **Effectuez** des requêtes http vers les serveurs web à partir des applications clientes correspondantes.
8. **Proposez** une access-list pour réaliser la liaison réseau extérieur-VLAN 10.
9. **Configurez** le routeur avec la proposition précédente.
10. **Testez** votre configuration pour un ping de PC1 ou PC3 vers PC2.
11. **Testez** votre configuration pour un ping de PC2 vers PC1 ou PC3
12. **Testez** une requête http vers le serveur SRV internet depuis PC1 ou PC3.
13. **Testez** votre configuration pour un ping entre PC2 et SRV1 ou SRV2.
14. **Proposez** une access-list pour réaliser la liaison VLAN30-VLAN 10.
15. **Configurez** le routeur avec la proposition précédente.
16. **Testez** votre configuration pour un ping de PC1 ou PC3 vers SRV1.
17. **Testez** votre configuration pour un ping de SRV1 ou SRV2 vers PC1