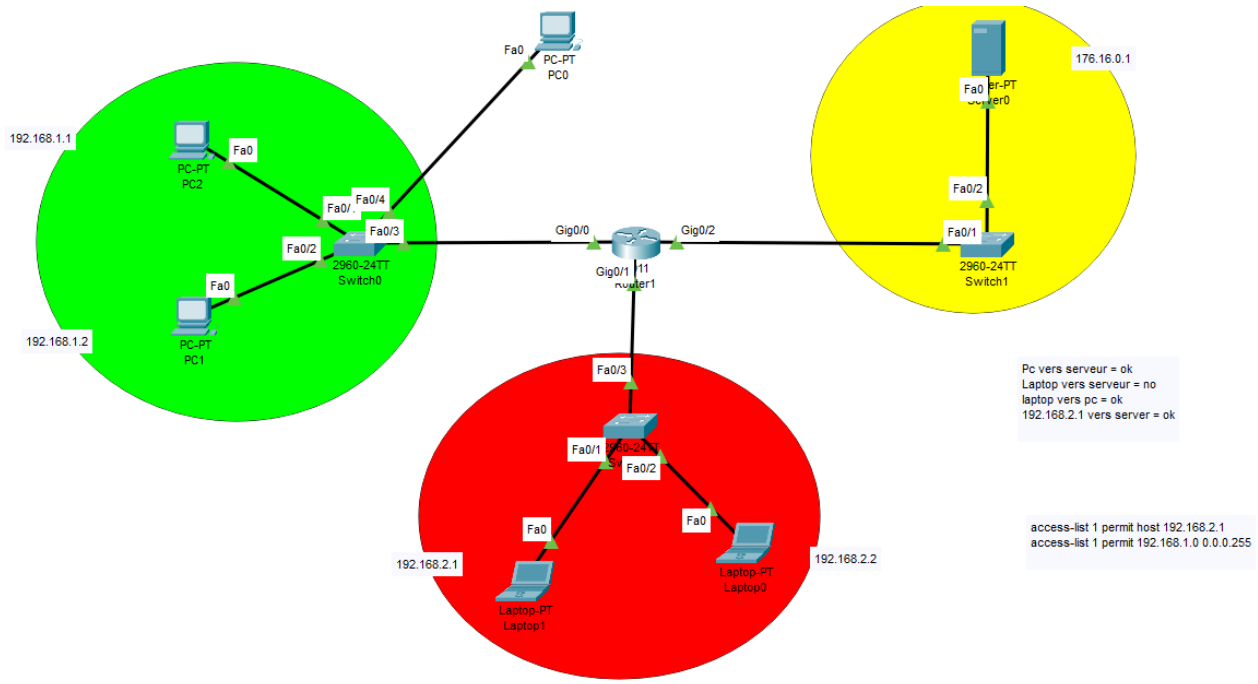
# TP - Configuration des Filtres ACL

Auteur : Adam Hakkam




Objectif :

L'objectif de ce TP est de configurer un filtre ACL sur un routeur Cisco dans Cisco Packet Tracer pour bloquer le trafic en provenance d'un hôte spécifique avec une adresse IP donnée.

Matériel utilisé :

- Un routeur central (Router1)
- Trois switches (un par VLAN)
- Plusieurs hôtes (PCs, Laptops, Serveur)
- Cisco Packet Tracer

Plan d'adressage :

# TP - Configuration des Filtres ACL

- VLAN Vert : 192.168.1.0/24

- VLAN Rouge : 192.168.2.0/24

- VLAN Jaune : 176.16.0.0/24

Étapes de Configuration :

1. Configuration de base sur Cisco Packet Tracer

   - Ajoutez les périphériques dans votre simulation.

   - Connectez les entre eux et vérifiez la connectivité.

2. Connexion au routeur

   - Accédez à la console via Cisco Packet Tracer.

3. Configuration de l'adresse IP du routeur

Router> enable

Router# configure terminal

Router(config)# interface GigabitEthernet0/0

Router(config-if)# ip address 12.0.0.1 255.0.0.0

Router(config-if)# no shutdown

Router(config-if)# exit

4. Création d'une ACL étendue

Router(config)# ip access-list extended Block_IP_12.0.0.100

Router(config-ext-nacl)# deny ip host 12.0.0.100 any

Router(config-ext-nacl)# permit ip any any

Router(config-ext-nacl)# exit

5. Application de l'ACL sur l'interface

Router(config)# interface FastEthernet0/0

Router(config-if)# ip access-group Block_IP_12.0.0.100 in

Router(config-if)# exit

6. Test avant l'application de l'ACL

- Effectuer un ping depuis PC0 vers PC1 :

PC0> ping 12.0.0.17

Reply from 12.0.0.17: bytes=32 time<1ms TTL=255

7. Test après application de l'ACL

PC0> ping 12.0.0.17

Request Timed Out

8. Vérification de l'ACL

Router# show access-lists

9. Suppression de l'ACL

Router(config)# interface FastEthernet0/0

Router(config-if)# no ip access-group Block_IP_12.0.0.100 in

Router(config-if)# exit

10. Test après suppression du filtre

# TP - Configuration des Filtres ACL

PC0> ping 12.0.0.17

Reply from 12.0.0.17: bytes=32 time<1ms TTL=255

Résumé de l'exercice sur ton scénario :

ACL utilisée :

access-list 1 permit host 192.168.2.1

access-list 1 permit 192.168.1.0 0.0.0.255

Comportements observés :

- PC vers serveur = OK
- Laptop vers serveur = BLOQUÉ
- Laptop vers PC = OK
- 192.168.2.1 vers serveur = OK

Conclusion :

Ce TP montre comment configurer une ACL étendue sur un routeur Cisco pour sécuriser le trafic réseau. En bloquant certains hôtes tout en autorisant d'autres, on affine les politiques de sécurité selon les besoins du réseau.