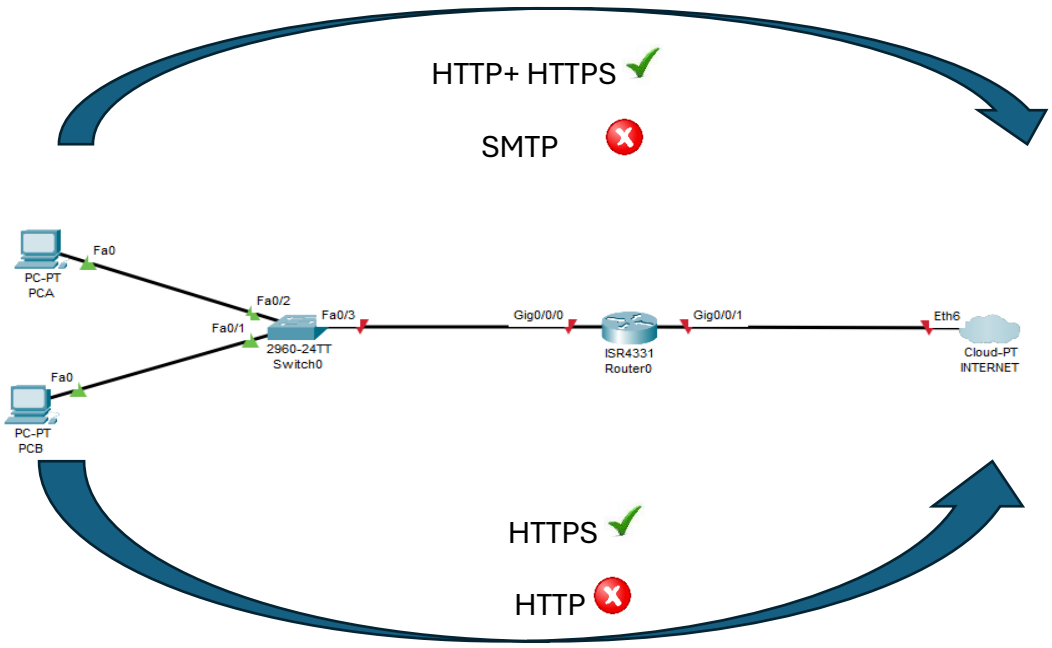
ACL

ACCES CONTROL LIST

Introduction

Les listes de contrôle d'accès (ACL) sont des outils essentiels en réseau permettant de gérer le trafic entrant et sortant sur les routeurs et les commutateurs. Elles permettent d'autoriser ou de bloquer certains types de trafic selon des critères définis.



Types d'ACL

Les ACL se divisent en deux grandes catégories :

1. ACL Standard

- Elles se basent uniquement sur l'adresse IP source pour filtrer le trafic.

- Plus simples à configurer, elles sont limitées en termes de précision.

- Exemples d'utilisation : Autoriser ou bloquer tout le trafic provenant d'une source spécifique.

2. ACL Étendue (Extended)

- Elles permettent de filtrer sur des critères plus complexes :

- Adresses IP source et destination.

- Protocole (TCP, UDP, ICMP, etc.).

- Numéros de port.

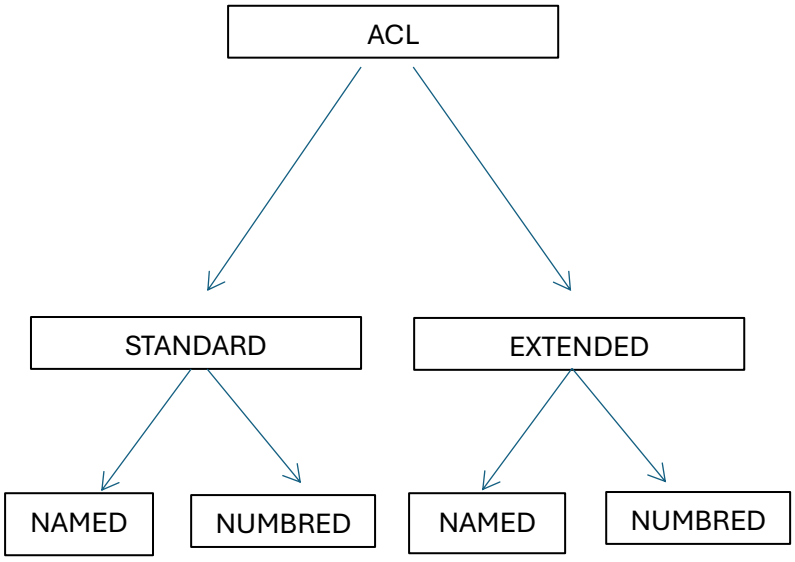
- Plus flexibles, elles offrent un contrôle granulaire sur le trafic

Nommées ou Numérotées ?

Les ACL peuvent être :

- Numérotées : Identifiées par un numéro (1 à 99 pour les ACL standards, 100 à 199 pour les ACL étendues).

- Nommées : Identifiées par un nom, offrant plus de lisibilité et facilitant la gestion



Configuration d'une ACL

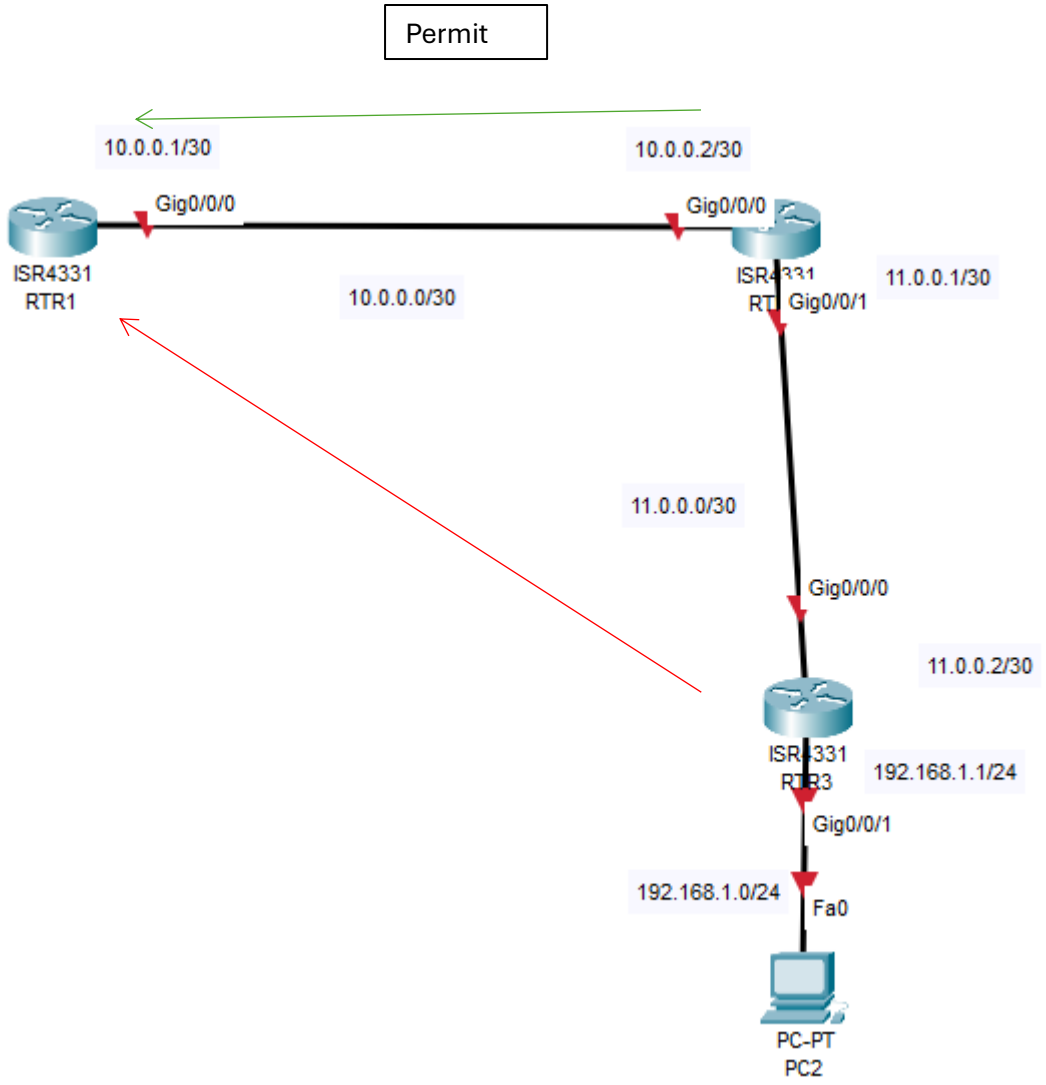
Voici les étapes principales pour configurer une ACL :

Exemple d'ACL Standard :

1. Création d'une ACL Standard :

R1(config)# access-list 1 permit host 10.0.0.2

R1(config)# access-list 1 deny host 10.0.0.3



La configuration des ACL dans cet exemple : permet la communication du Routeur 2 vers le routeur 1, mais empêche la communication entre le réseau passant par le routeur 3.

Configuration OSPF :

R2(config)# router ospf 1

R2(config)# net 10.0.0.0 0.0.0.3 Area 0

R2(config)# net 11.0.0.0 0.0.0.3 Area 0

R1(config)# router ospf 1

R1(config)# net 10.0.0.0 0.0.0.3 Area 0

R3(config)# router ospf 1

R1(config)# net 11.0.0.0 0.0.0.3 Area 0

Configuration ACL

R1(config)# Access-list ?

R1(config)# <1-99> IP standard Access list

<100-199>IP extended Access list

R1(config)# Access-list 1 permit host 10.0.0.2

R1(config)# Access-list 1 deny host 11.0.0.2

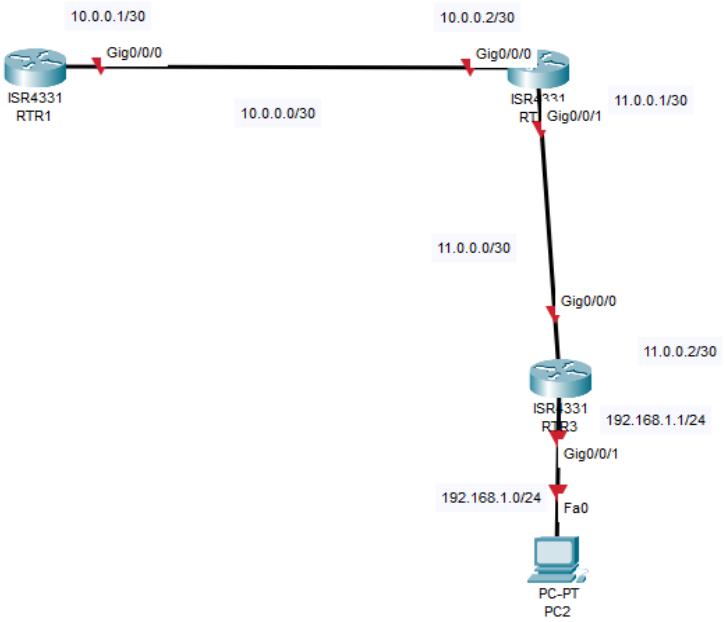
R1(config)# int G0/0/0

R1(config-if)# ip access-group 1 in

Vérification :

R1# show access-list

2. Création d'une ACL Etendue :



Dans ce cas nous allons permettre la connexion a distance via telnet du R1 vers R2, et empêcher le ping. Cependant empêcher telnet de R3 vers R2 et permettre le ping.

#Permettre le passage pour Telnet

R2(config)# Access-list 100 permit tcp host 10.0.0.1 host 10.0.0.2 eq 23

#Empecher les ping

R2(config)# Access-list 100 Deny icmp host 10.0.0.1 host 10.0.0.2 echo

#Application à une interface

R2(config)#int G0/0/0

R2(config-if)#ip access-group 100 in

Empêcher la connexion telnet depuis le réseau 11.0.0.0/30

R2(config)#access-list 101 deny tcp 11.0.0.0 0.0.0.3 host 11.0.0.1 eq 23

#Autoriser le ping

R2(config)#access-list 101 permit icmp host 11.0.0.2 host 11.0.0.1 echo

#Application à une interface

R2(config)#access-list 101 permit ospf any any

R2(config)#int G0/0/1

R2(config-if)#ip access-group 101 in

3. Création d'une ACL Nommée :

R1(config)#ip access-list standard TEST1

R1(config-std-nacl)#permit host 10.0.0.2

R1(config-std-nacl)#deny host 11.0.0.2

R1(config-std-nacl)#int G0/0/0

R1(config-if)#ip access-group TEST1 in