#CR4

ACL

RAPPEL DE NOTION IMPORTANT

EN-tête IPV4

En-tête IPv4

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Version d'IP				Longueur de l'en-tête				Type de service								Longueur totale															
Identification																Indicateur			Fragment offset											
Durée de vie								Protocole								Somme de contrôle de l'en-tête															
Adresse source																															
Adresse destination																															
Option(s) + remplissage																															

- quelques infos intérsant:
  i. longueur totale: 16 bits donc 2^16=65535
  ii. longueur d'en-tête 32 bits * 8 * 5 = 20 bytes
  iii. notion de MTU = 1500(culture générale approfondie) donc on a Identification Indicateur et Fragment offset pour distinguer des parquets géants et le regrouper après. Mais on ne fait pas ça généralement pour la performance du réseau.

calcul de masque générique

- tous les chiffres dans le masque normal sont la conbinaison de 2^0 à 2^7.(1 2 4 8 16 32 64 128)
- le masque générique est le résultat de soustraition entre le masque normal et 255.

Notion ACL

3 types de ACL

1. standard 1-99 modification nest pas autorisé
2. extended 100-199 modification nest pas autorisé
3. named ****(plus flexible) on peut le modifier plus facilement

Comment fonctionne ACL

ACL est un ensemble de règles, qui est appliqué à une certaine interface du routeur. Pour les interfaces de routeur, la liste de contrôle d'accès a deux directions:

Out: Un paquet de données qui a été traité par le routeur et quitte l'interface du routeur.

In: Le paquet de données qui a atteint l'interface du routeur sera traité par le routeur.

Si une liste de contrôle d'accès est appliquée à une interface, c'est-à-dire qu'un ensemble de règles est appliqué à l'interface, le routeur appliquera l'ensemble de règles au paquet de données pour une inspection séquentielle.

1. Si la première règle correspond, aucune autre inspection ne sera effectuée et le routeur décidera d'autoriser ou de rejeter le paquet de données.
2. S'il ne correspond pas à la première règle, effectuez une vérification séquentielle jusqu'à ce qu'il y ait une correspondance de règle, et le routeur décidera si le paquet de données va être autorisé ou rejeté.
3. Si aucune règle ne correspond à la fin, le routeur rejettera le paquet de données selon la règle par défaut.(c'est à dire tous les règles vont terminé par une phase 'deny any')

Cela montre que les paquets de données sont autorisés ou rejetés.

'Router (config) # access-list access-list-number {permit | deny} source [source-wildcard]'

access-list-number: numéro de table de la liste de contrôle d'accès. Pour les listes de contrôle d'accès standard, le numéro de table est un nombre compris entre 1 et 99.

permit | deny: si les conditions de test sont remplies, le flux de communication va être autorisé ou être refusé

source: l'adresse source du paquet de données, qui peut être une adresse d'hôte ou une adresse réseau.

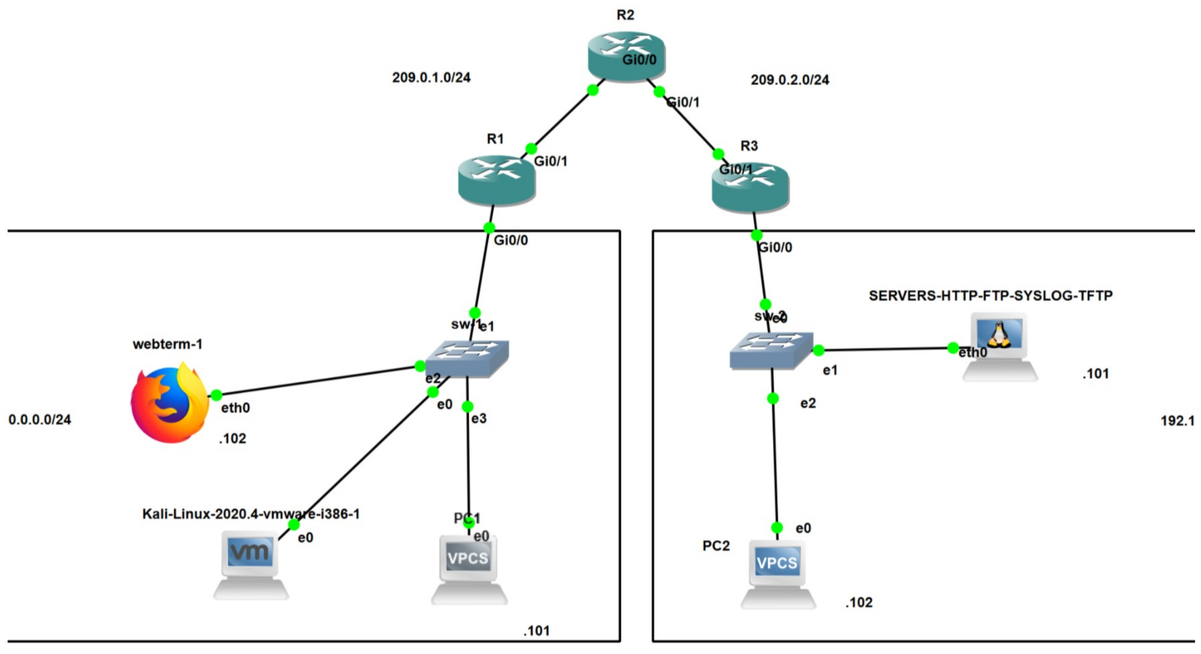
source-wildcard: masque générique.

points importants

- l'appliquer sur une interface après la configuration.
- lt (inférieur à), gt (supérieur à), eq (égal à), neq (différent de) un numéro de port.
- *established* n'est que pour les paquets TCP. C'est parce que TCP a three-way handshake. après la connexion est 'established. et les marques *ACK* et *RST* vont être changé pour le dire.

Si l'on veut permettre des paquets sous protocol TCP, il faut ajouter 'permit any IP-destination willcard-destination established'

TOPOLOGIE SPECIAL



pour la route par defaut depuis toolbox

'route add default gw 10.0.0.1'

ou bien

'ip route add default via 10.0.0.1 dev eth0'

contourler ACL

'nmap -e eth0 -S IP(clinquant) IP(BUT)''

nmap.org