Mohamed Droussi

Alexandre Samperez

Adem Grira

RAPPORT SAE 21

Construire un réseau info. pour une petite structure

Sommaire :

Cahier des charges

L'objectif est de concevoir un réseau d'entreprise typique pour une PME, structuré autour d'un **switch multi-couche (MLS)** jouant le rôle de cœur de réseau. Ce MLS assure la commutation et le routage pour plusieurs **VLANs** : deux pour les services internes (ex. RH et ingénierie) et un pour les **serveurs internes**.

Le MLS est relié à un **pare-feu Cisco ASA**, qui :

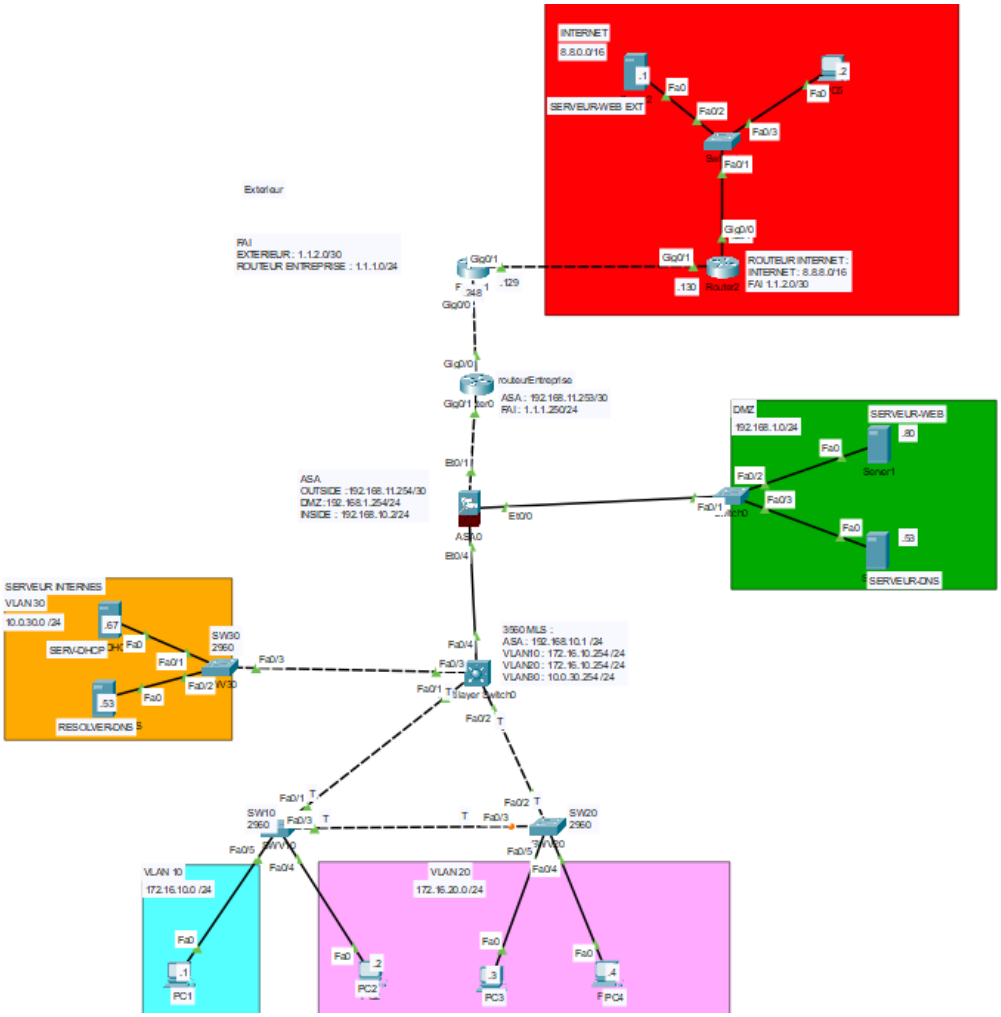
- Autorise l'accès au **serveur Web en DMZ** uniquement via les ports **80 et 443 (TCP)**.
- Vérifie que les réponses d'Internet correspondent à des connexions initiées depuis l'intérieur.

Un **FAI** fournit :

- Une **plage d'adresses publiques** au routeur d'entreprise.
- Du **NAT overload** pour les VLANs 10 et 20, et du **NAT statique** pour le serveur Web en DMZ.

Enfin, un réseau externe de test permet de valider l'accès à Internet depuis les machines internes, ainsi que l'accessibilité du serveur Web de l'entreprise

Plan d’adressage :



Etape 1 : Construction de coeur de réseau avec les switches d’accès et le Multi-layer switch (/5)

Voici la configuration du SW10 qui relie la vlan10 et la vlan 20

```
hostname SWV10
!
!
!
no ip domain-lookup
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/2
 switchport access vlan 10
 switchport mode access
!
interface FastEthernet0/3
 switchport trunk allowed vlan 10,20
 switchport mode trunk
!
interface FastEthernet0/4
 switchport access vlan 20
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 10
 switchport mode access
```

On a configuré le port Fa0/1 en mode trunk pour transporter plusieurs vlan(Ici on a la Vlan 10 et 20)

Voici la configuration du switch MLS(on a activé le ip routing) :

```
interface FastEthernet0/1
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/2
 switchport trunk allowed vlan 10,20
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
interface FastEthernet0/3
 switchport access vlan 30
 switchport mode access
!
interface FastEthernet0/4
 no switchport
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
```

Les interfaces Fa0/1 et Fa0/2 ont été configurées en mode trunk avec l'encapsulation 802.1Q (dot1q), afin de permettre le transport simultané de plusieurs VLANs sur un même lien physique. Cette configuration assure la transmission des VLANs 10 et 20 vers d'autres switches comme SW10 et SW20, facilitant ainsi la communication entre les différents VLANs du réseau.

Etape 2 : Ajout de l'ASA et du service DHCP (/5)

Configuration du firewall ASA :

```
hostname ciscoasa
names
!
interface Ethernet0/0
 switchport access vlan 3
!
interface Ethernet0/1
 switchport access vlan 2
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Ethernet0/4
!
interface Ethernet0/5
!
interface Ethernet0/6
!
interface Ethernet0/7
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.10.2 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 192.168.11.254 255.255.255.252
!
interface Vlan3
 no forward interface Vlan1
 nameif DMZ
 security-level 50
 ip address 192.168.1.254 255.255.255.0
!
!
route outside 0.0.0.0 0.0.0.0 192.168.11.253 1
route inside 172.16.0.0 255.255.0.0 192.168.10.1 1



access-list autorisation extended permit tcp any host 192.168.1.80 eq www
access-list autorisation extended permit tcp any host 192.168.1.80 eq 443
access-list autorisation extended permit udp any host 192.168.1.53 eq domain
access-list autorisation_DMZ extended permit icmp any any
!
!
access-group autorisation in interface outside
!
!
class-map inspection
 match default-inspection-traffic
!
policy-map global
 class inspection
  inspect icmp
policy-map intoDMZ
 class inspection
  inspect http
!
service-policy global interface outside
service-policy intoDMZ interface DMZ
service-policy intoDMZ interface inside
!
telnet timeout 5
ssh timeout 5
!
dhcpd auto_config outside
!
dhcpd enable inside
```

On a tout d'abord configuré trois vlans :

- Vlan1 (inside) – Niveau de sécurité 100
  Adresse IP : 192.168.10.2/24
  Connecté au réseau interne (poste client, serveurs internes)

- Vlan2 (outside) – Niveau de sécurité 0
  Adresse IP : 192.168.11.254/30
  Relié au routeur d'accès Internet (fournisseur d'accès)

- Vlan3 (DMZ) – Niveau de sécurité 50
  Adresse IP : 192.168.1.254/24
  Réseau intermédiaire accueillant le serveur Web accessible depuis Internet

Ensuite on a crée différentes ACL :

La première ACL autorise l'accès http et HTTPS au serveur Web en DMZ

La deuxième autorise le trafic DNS

La troisième permet le ping a travers la DMZ

L'ACL est appliquée sur l'interface outside

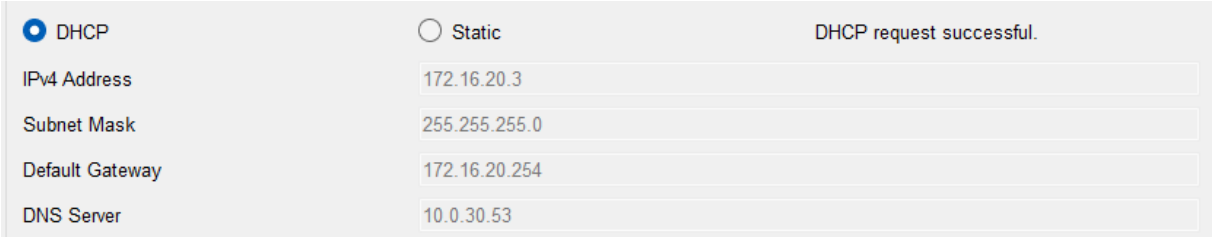
On a aussi mis en place des politiques d'inspection afin de suivre l'etat des connexions :

- L'inspection ICMP permet de suivre les requêtes ping.
- L'inspection HTTP est appliquée au trafic entre les zones inside et DMZ.

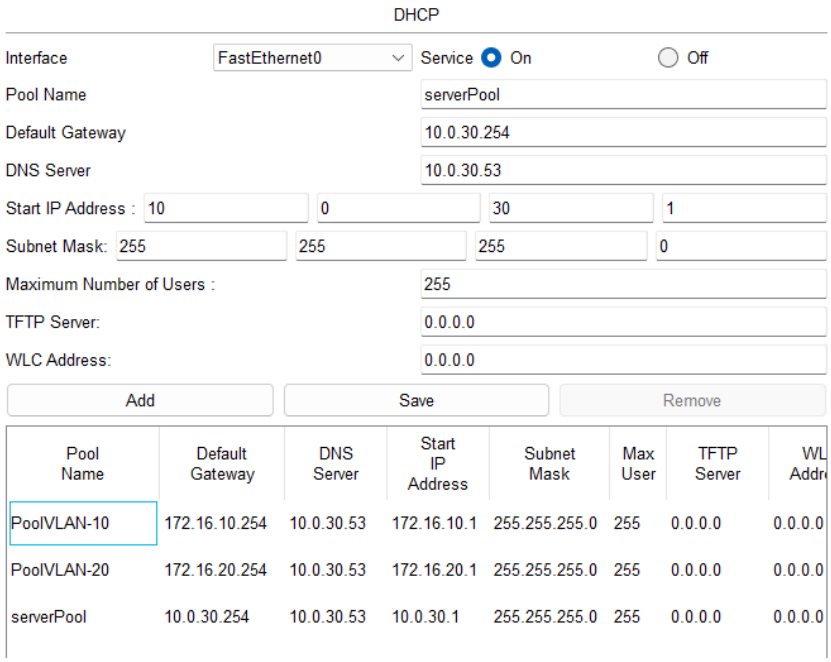
Ensuite on les a appliqués sur les interfaces concernées.

Pour ce qui est du routage on a d'abord defini une route par defaut vers le routeur internet

, on a defini une route pour les sous réseaux internes et on a activé le DHCP pour les machines internes :



Configuration Serveur DHCP :

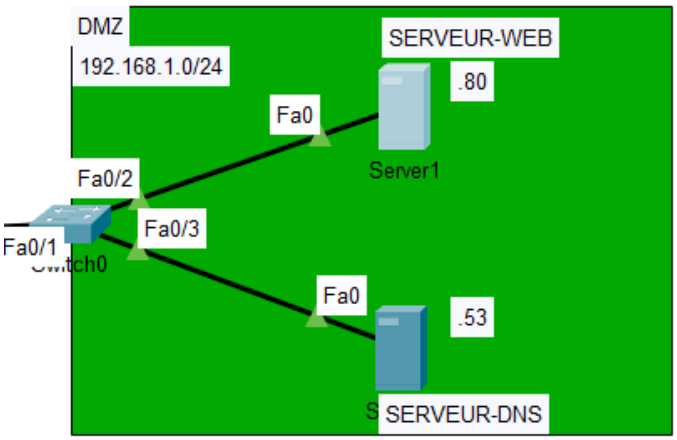


Etape 3 : Ajout de la DMZ et du routeur du FAI (/10)

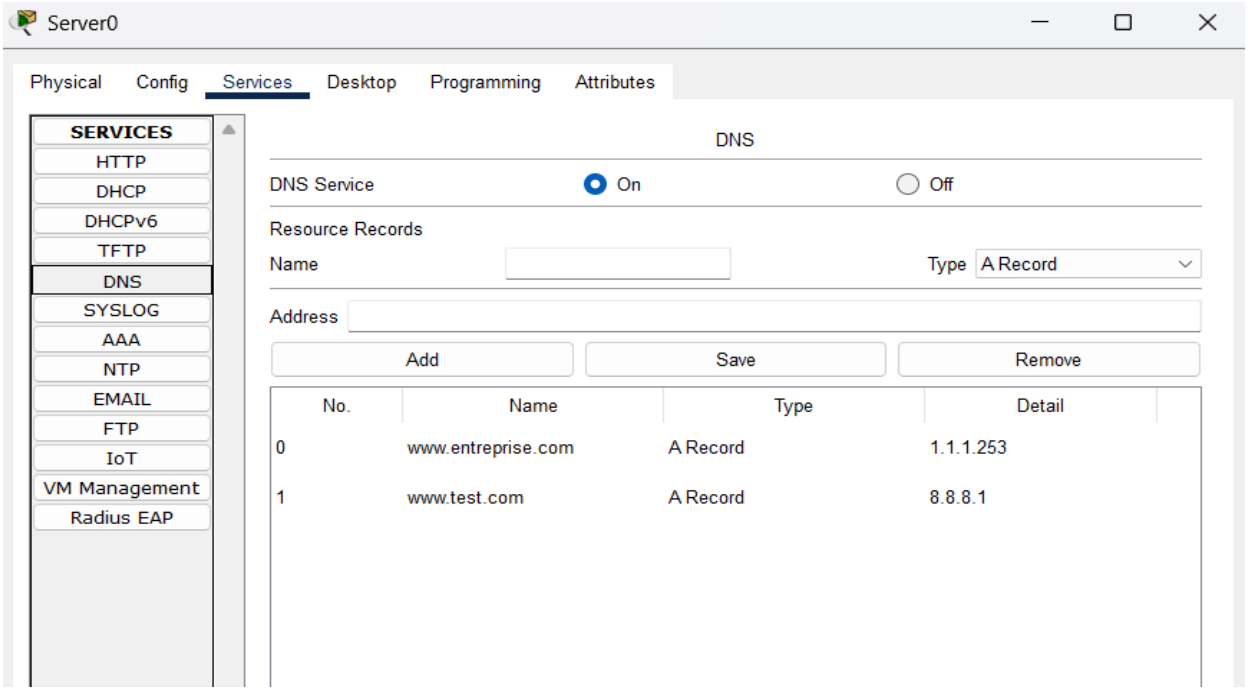
Cette étape a pour but d'intégrer une DMZ (zone démilitarisée) au sein du réseau de l'entreprise, afin d'y héberger un serveur Web accessible depuis l'extérieur via Internet. Elle comprend également la mise en place d'un routeur FAI, qui assure la traduction d'adresses (NAT) pour permettre :

- L'accès externe au serveur Web de la DMZ via une IP publique (NAT statique),
- La navigation Internet des clients internes (NAT dynamique overload),
- La sécurisation des flux à l'aide du pare-feu ASA.

Schema topologique de le DMZ :



Configuration du serveur DNS de la DMZ :



Règles définies afin que la serveur de la DMZ soit accessible sur les bons ports :

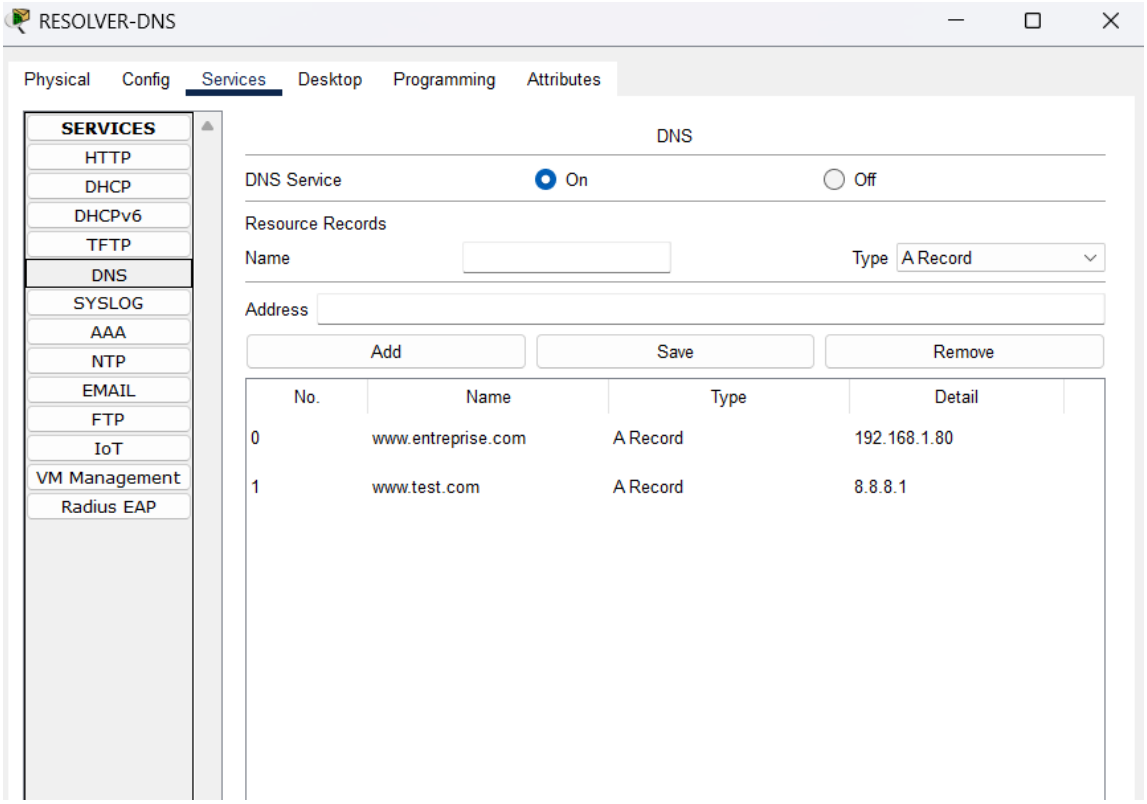
```
access-list autorisation extended permit tcp any host 192.168.1.80 eq www
access-list autorisation extended permit tcp any host 192.168.1.80 eq 443
```

NAT dynamique (overload) :

```
ip nat pool local 1.1.1.250 1.1.1.250 netmask 255.255.255.0
ip nat inside source list 1 pool local overload
```

On a tout d'abord crée un pool avec une seule addresse IP(1.1.1.250), ensuite on a utilisée la surcharge NAT(PAT) pour permettre a plusieurs machines internes d'utiliser une seule IP publique.

Serveur DNS du réseau interne :



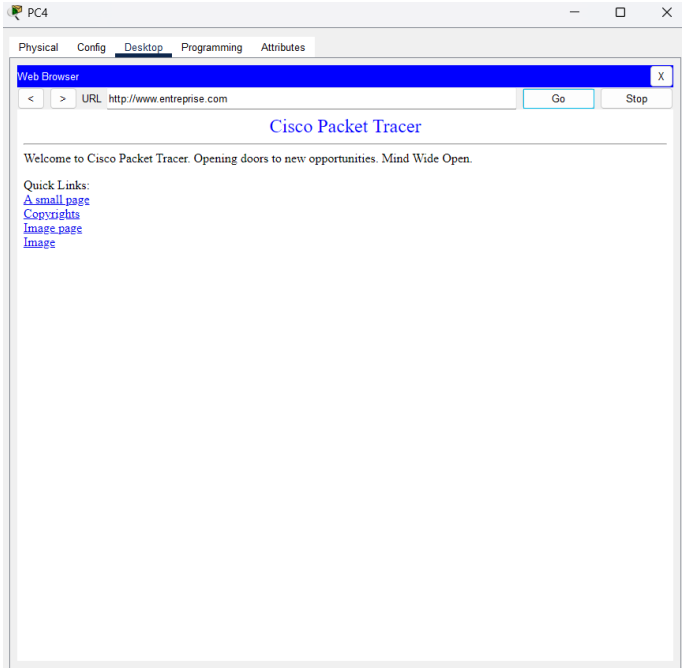
On peut y voir la DMZ (192.168.1.80) et le réseau extérieur (8.8.8.1)

Configuration du routeur FAI avec mise en place du NAT statique :

```
interface GigabitEthernet0/0
 ip address 1.1.1.250 255.255.255.0
 ip nat outside
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 192.168.11.253 255.255.255.252
 ip nat inside
 duplex auto
 speed auto

ip nat pool local 1.1.1.250 1.1.1.250 netmask 255.255.255.0
ip nat inside source list 1 pool local overload
ip nat inside source static tcp 192.168.1.80 80 1.1.1.253 80
ip nat inside source static tcp 192.168.1.80 443 1.1.1.253 443
ip nat inside source static udp 192.168.1.53 53 1.1.1.252 53
ip classless
ip route 192.168.0.0 255.255.0.0 192.168.11.254
ip route 172.16.0.0 255.255.0.0 192.168.11.254
```

Test de connectivité (en http) entre le réseau interne et la DMZ :



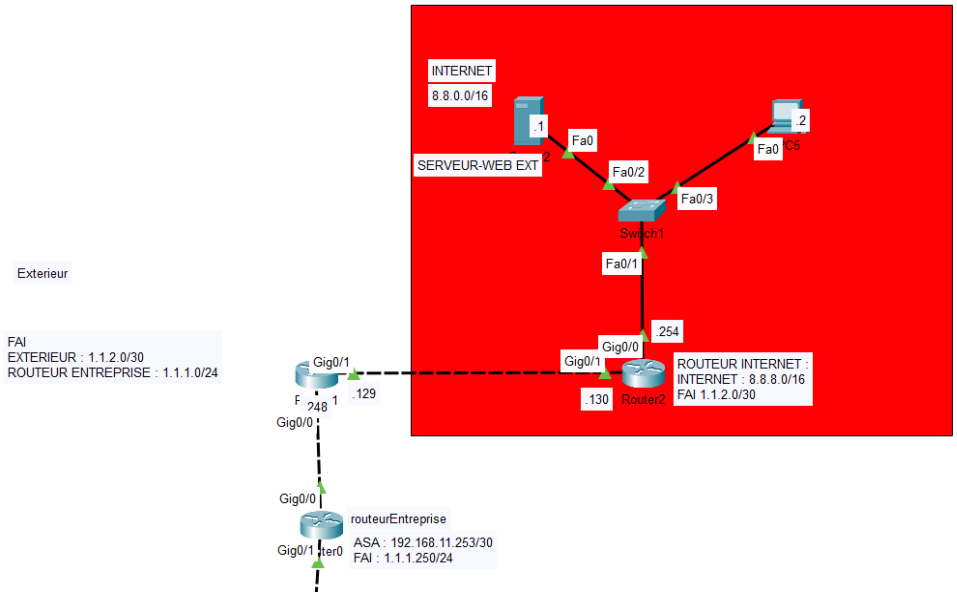
On peut donc voir a ce stade de la manipulation que je peux joindre la DMZ depuis mon reseau interne sans problème grâce aux règles défini dans le firewall ASA et la configuration du NAT statique et dynamique.

Etape 4 : Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI (/5)

Objectifs de cette dernière étape

- Créer un réseau externe public (8.8.0.0/16) contenant :
    - Un serveur Web externe (pour www.test.com)
    - Un client Internet (pour tester l'accès au serveur Web de l'entreprise)
- Interconnecter ce réseau avec l'entreprise via le FAI, grâce à un réseau de transit 1.1.2.0/30
- Assurer la résolution DNS côté Internet et le routage dynamique EIGRP entre le FAI et le routeur "Internet".

Schéma topologique du réseau publique(8.8.0.0/16) avec le FAI :



-Zone rouge : réseau public 8.8.0.0/16

- Serveur Web externe 8.8.8.1 (Fa0)
- Client Internet 8.8.8.2 (Fa0)
- Routeur "Internet":
    - Interface G0/0 : 8.8.8.254
    - Interface G0/1 : 1.1.2.130 (vers FAI)

- Interconnexion avec le FAI

- Routeur FAI :
    - Interface G0/1 : 1.1.2.129/30 (vers Routeur Internet)
    - Interface G0/0 : 1.1.1.248/24 (vers entreprise)

Configuration du routage dynamique EIGRP sur les trois routeurs (FAI, RouteurEntreprise et Routeur Internet) :

Routeur FAI :

```
router eigrp 100
 network 1.1.2.128 0.0.0.3
 network 1.1.1.0 0.0.0.255
```

RouteurEntreprise :

```
router eigrp 100
 network 1.1.1.0 0.0.0.255
```

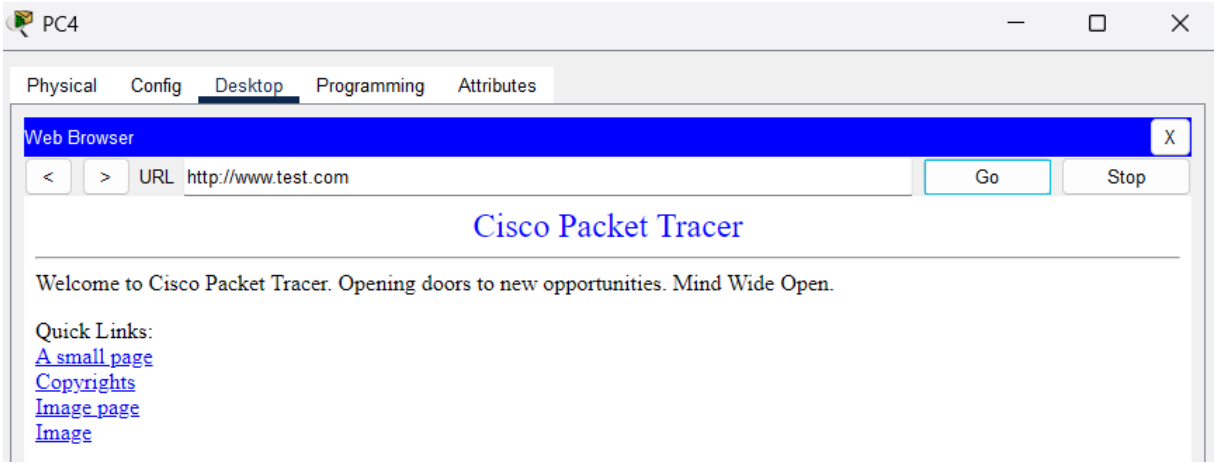
RouteurInternet :

```
router eigrp 100
 network 8.8.0.0 0.0.255.255
 network 1.1.2.128 0.0.0.3
```

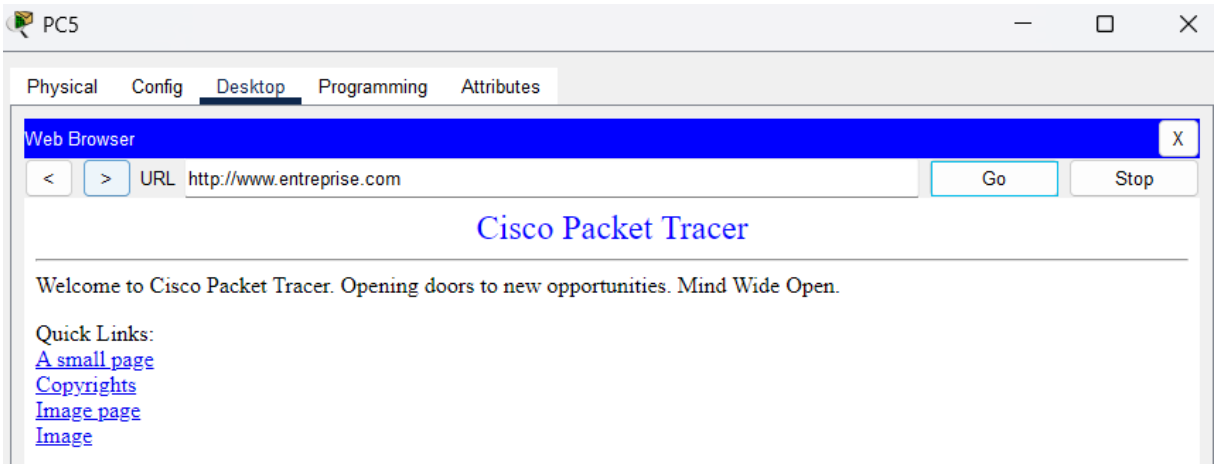
Cela va permettre a chaque routeur de reconnaitre le reseau de l'autre.

Tests ultimes :

Ping d'une machine du reseau interne en http le nom de domaine www.test.com qui correspond au reseau externe 8.8.8.1 :



Ping de la machine externe du reseau externe en http avec le nom de domaine www.entreprise.com qui correspond au serveur web de la DMZ :



Conclusion

Au terme de cette SAE, nous avons conçu et déployé l'infrastructure réseau complète d'une petite entreprise, en répondant aux exigences de connectivité, de sécurité et d'accès externe. Chaque étape a permis d'introduire des concepts clés : segmentation en VLANs, routage avec MLS, pare-feu ASA, DMZ, NAT statique et dynamique, ainsi que le routage inter-domaines via EIGRP.

Les tests finaux ont confirmé le bon fonctionnement du réseau :

- Les clients internes accèdent correctement aux ressources Internet,
- Le serveur Web de la DMZ est accessible depuis l'extérieur uniquement sur les ports autorisés,
- Le trafic est correctement filtré par le pare-feu.