SAÉ 21 – Construire un réseau informatique pour une petite entreprise

Rapport d'avancement détaillé avec commentaires

Préparé par :

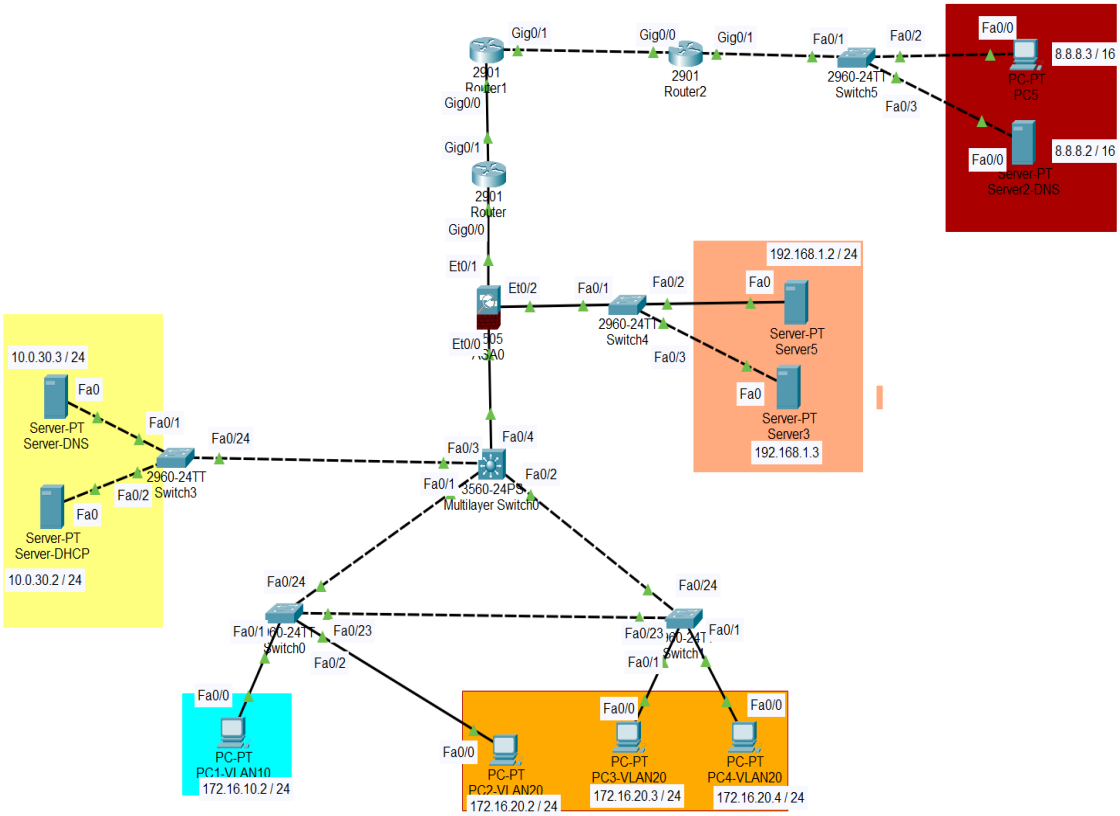
- BIN ARIFFIN Muhammad Farihin
- AYED Sofian
- GHAZEL Adam

Introduction

Dans le cadre de la SAÉ 21, nous avons été amenés à construire l'architecture réseau

d'une petite entreprise fictive.
L'objectif était de concevoir une infrastructure cohérente, segmentée par services à l'aide de VLANs, d'assurer leur interconnexion via un MLS, de sécuriser les flux grâce à un pare-feu ASA, d'intégrer des services DHCP et DNS, et de rendre un serveur Web accessible depuis Internet à travers une DMZ.
Le présent document détaille chaque étape de la mise en œuvre avec les commandes utilisées, les explications associées et les choix techniques justifiés.

Plan d'adressage IP



Étape 1 – Construction de cœur de réseau avec les switches d'accès et le Multi-layer switch

Objectif : Créer une segmentation logique à l'aide de VLANs, permettre la communication entre eux et structurer la topologie autour d'un MLS (switch de niveau 3).

Les différents équipements réseaux :

- 1 MLS 3560
- 3 Switch 2960
- 3 PC sur VLAN 20
- 1 PC sur VLAN 10
- Serveur DNS et DHCP sur VLAN 30

Nous avons attribué des adresses IP statiques à chaque équipement dans chaque VLAN en utilisant un masque de sous-réseau /24, soit 255.255.255.0. Ce format permet d'avoir 254 adresses IP par VLAN.

- VLAN 10 : 172.16.10.0 avec gateway de 172.16.10.1
- VLAN 20 : 172.16.20.0 avec gateway de 172.16.20.1
- VLAN 30 : 10.0.30.0 avec gateway de 10.0.30.1

Configuration du MLS :

Création des VLANs :

```
MLS(config)# vlan 10
MLS(config-vlan)# name Vlan10
MLS(config)# vlan 20
MLS(config-vlan)# name Vlan20
MLS(config)# vlan 30
MLS(config-vlan)# name Vlan 30
```

Configuration des interfaces VLAN pour activer le routage inter-VLAN :

Pour que les différents VLAN puissent communiquer entre eux, nous avons configuré des interfaces VLAN sur le MLS. Chacune de ces interfaces représente la gateway pour les machines d'un VLAN :

```
MLS(config)# interface vlan 10
MLS(config-if)# ip address 172.16.10.1 255.255.255.0
MLS(config-if)# no shutdown

MLS(config)# interface vlan 20
MLS(config-if)# ip address 172.16.20.1 255.255.255.0
MLS(config-if)# no shutdown
```

```
MLS(config)# interface vlan 30
MLS(config-if)# ip address 10.0.30.1 255.255.255.0
MLS(config-if)# no shutdown
```

Activation du routage inter-VLAN :

```
MLS(config)# ip routing
```

STP (Spanning Tree Protocol) : priorité basse sur le MLS pour qu'il soit racine :

```
MLS(config)# spanning-tree vlan 10,20,30 priority 4096
```

Configuration trunk entre le MLS et les switches d'accès :

```
MLS(config)# interface fa0/1
MLS(config)# switchport trunk encapsulation dot1q
MLS(config-if)# switchport mode trunk
MLS(config-if)# switchport trunk allowed vlan 10,20,30

MLS(config)# interface fa0/2
MLS(config-if)# switchport mode access vlan 20
MLS(config-if)# switchport mode access

MLS(config)# interface fa0/3
MLS(config-if)# switchport mode access vlan 30
MLS(config-if)# switchport mode access
```

<u>Configuration des switchs :</u>

Switch 0 :

```
Switch0(config)# vlan 10
Switch0(config-vlan)# vlan 20
Switch0(config-vlan)# vlan 30

Switch0(config)# interface fa0/1
Switch0(config-if)# switchport access vlan 10
Switch0(config-if)# switchport mode access

Switch0(config)# interface fa0/2
Switch0(config-if)# switchport access vlan 20
Switch0(config-if)# switchport mode access
```

```
Switch0(config)# interface fa0/23
Switch0(config-if)# switchport access vlan 20
Switch0(config-if)# switchport trunk native vlan 10
Switch0(config-if)# switchport trunk allowed vlan 10,20
Switch0(config-if)# switchport mode access

Switch0(config)# interface fa0/24
Switch0(config-if)# switchport access vlan 10

Switch0(config-if)# switchport mode access
```

Switch 1:

```
Switch1(config)# vlan 10
Switch1(config-vlan)# vlan 20
Switch1(config-vlan)# vlan 30

Switch1(config)# interface fa0/1
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# switchport mode access

Switch1(config)# interface fa0/2
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# switchport mode access

Switch1(config)# interface fa0/23
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# switchport trunk native vlan 10
Switch1(config-if)# switchport trunk allowed vlan 10,20
Switch1(config-if)# switchport mode access

Switch1(config)# interface fa0/24
Switch1(config-if)# switchport access vlan 20
Switch1(config-if)# switchport mode access
```

Switch 3:

```
Switch3(config)# vlan 10
Switch3(config-vlan)# vlan 20
Switch3(config-vlan)# vlan 30
```

Switch3(config)# interface fa0/1
Switch3(config-if)# switchport access vlan 30
Switch3(config-if)# switchport mode access

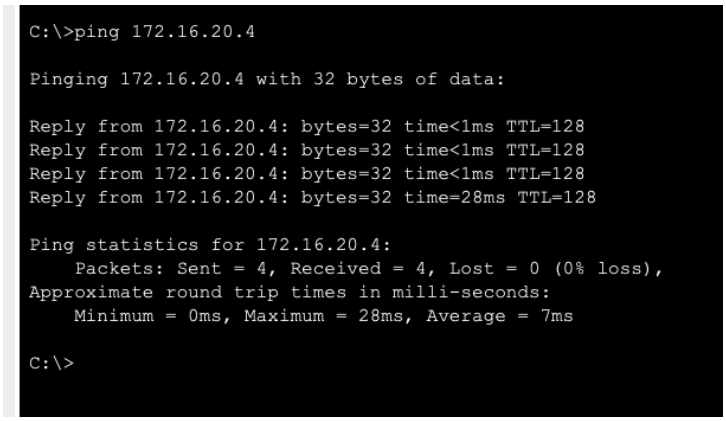
Switch3(config)# interface fa0/2
Switch3(config-if) switchport access vlan 30
Switch3(config-if) switchport mode access

Switch3(config)# interface fa0/3
Switch3(config-if) switchport access vlan 30
Switch3(config-if) switchport mode access

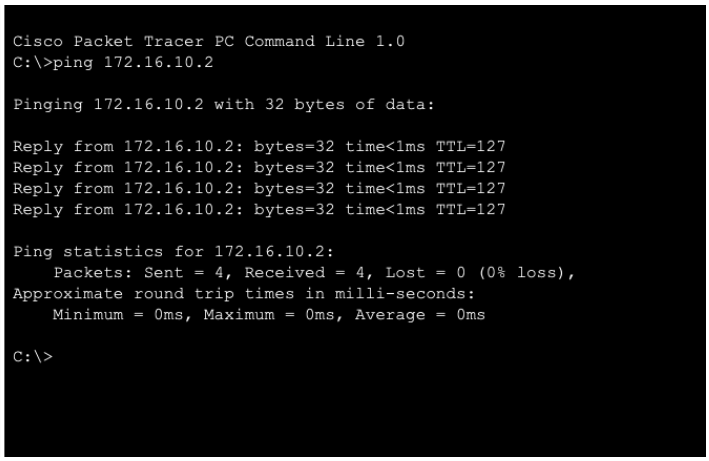
Switch3(config)# interface fa0/24
Switch3(config-if) switchport access vlan 30
Switch3(config-if) switchport mode access

Test ping pour vérifier la connectivité :

Depuis PC3 vers PC4 (sur même VLAN) :



Depuis PC4 vers PC1 (sur difference VLAN) :



Étape 2 – Ajout de l'ASA et du service DHCP

Objectif : Permettre l'attribution automatique des adresses IP et la résolution des noms de domaines internes.

Configuration de l'interface VLAN côté ASA pour le réseau interne :

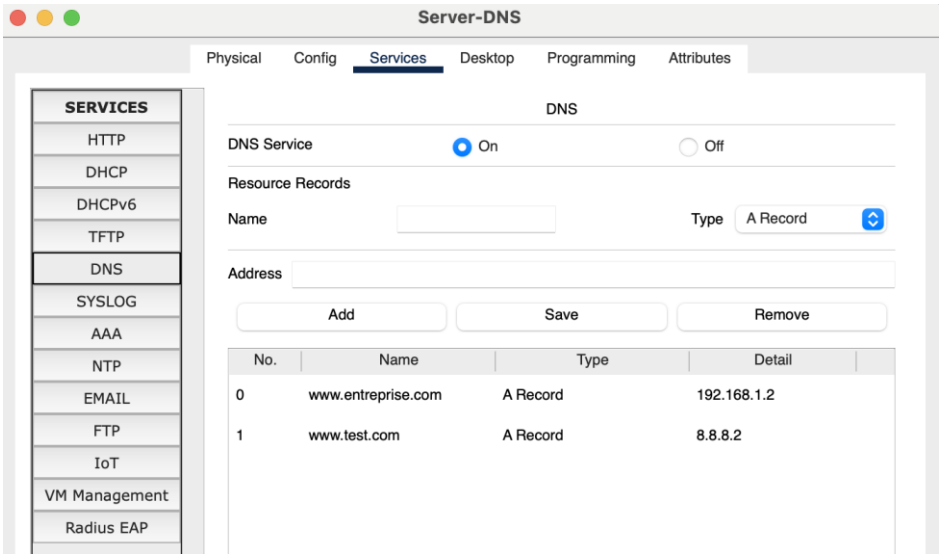
```
ASA(config)# interface vlan 1
ASA(config-if)# nameif inside
ASA(config-if)# security-level 100
ASA(config-if)# ip address 192.168.10.2 255.255.255.252
ASA(config-if)# no shutdown

ASA(config)# interface ethernet0/0
ASA(config-if)# switchport access vlan 1
```

La configuration de DNS :

Elle permet de traduire des noms de domain tels que www.entreprise.com et www.test.com en l'adresse IP correspondante.

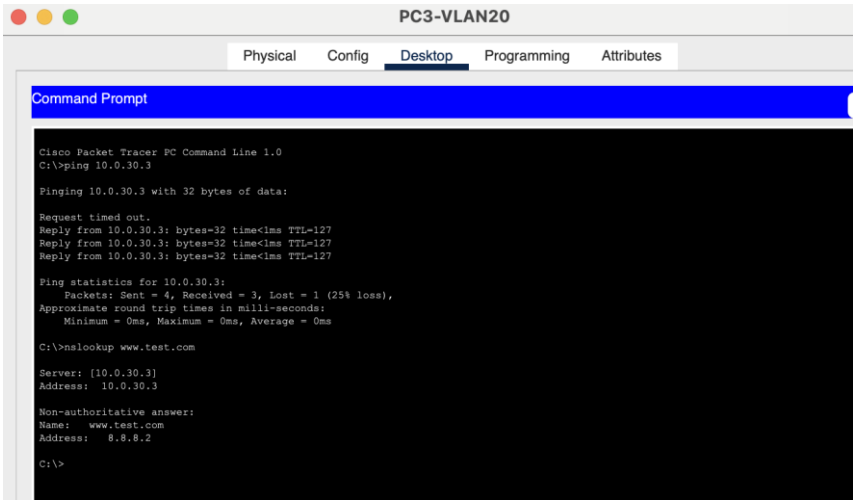
DNS interne – Résolution locale sur le serveur (onglet Services > DNS) :

- Nous avons allumer le DNS Service.
- Nous avons aussi entrée les noms de domain de www.entreprise.com et www.test.com avec l'adresse IP correspondante.
- On décide l'enregistrement de type A car il redirige directement un nom d'hôte vers une adresse IP numérique.



Vérification sur un client :

- ping 10.0.30.3
- nslookup www.test.com



La configuration de DHCP :

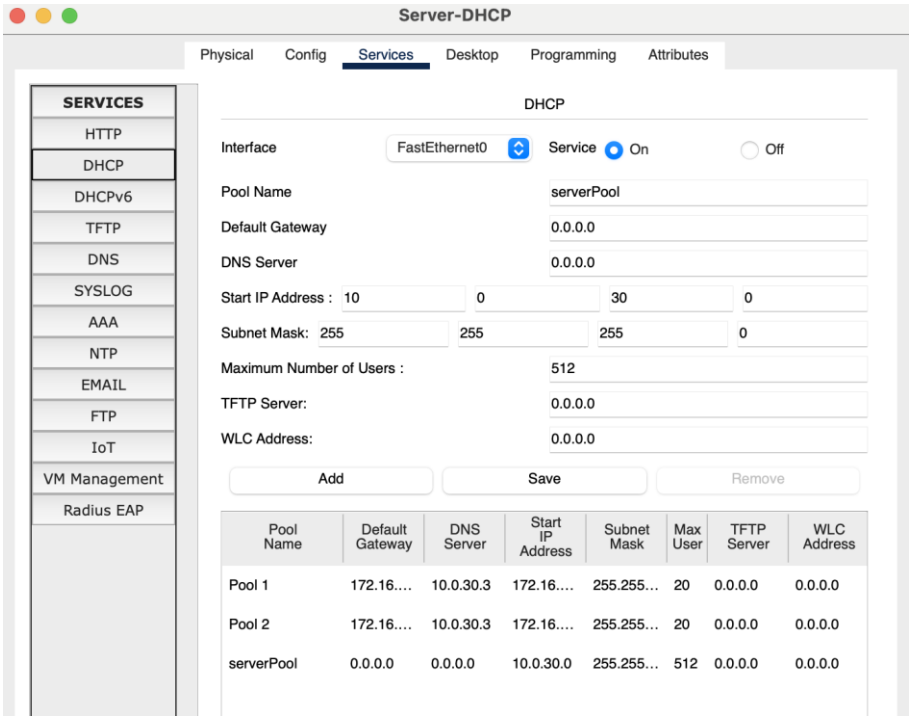
Sur le MLS, il faut configurer de “ IP helper address ”. Il utilise sur les périphériques réseau (généralement des routeurs ou des commutateurs de couche 3) pour transférer certains types de trafic de diffusion d'un sous-réseau (VLAN) à un autre — le plus souvent des requêtes DHCP.

MLS(config)# interface vlan 10
MLS(config-if)# ip helper-address 10.0.30.2

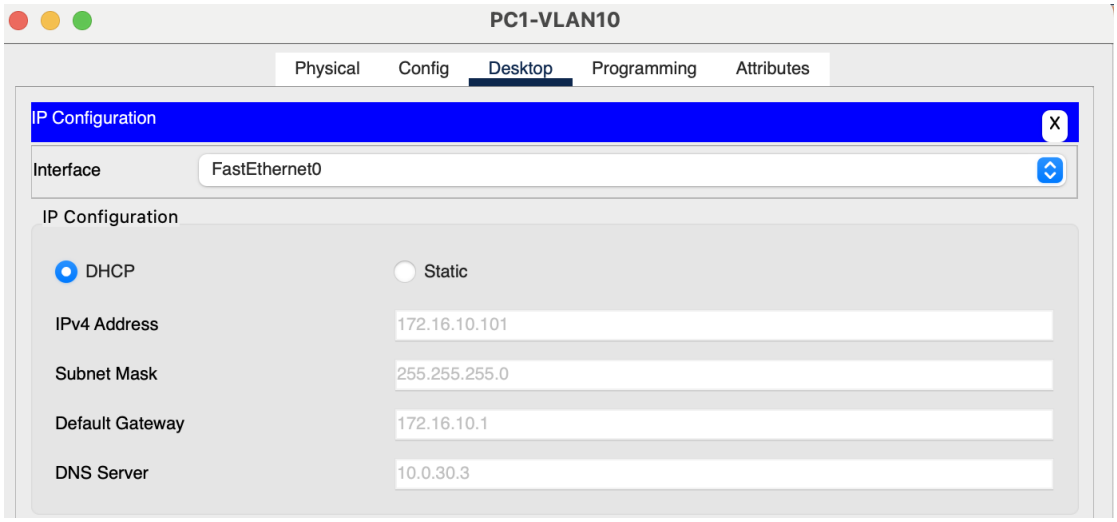
MLS(config)# interface vlan 20
MLS(config-if)# ip helper-address 10.0.30.2

Sur le serveur DHCP :

Nous avons configuré le service DHCP en définissant trois pools distincts pour chaque VLAN, avec une plage d'adresses allant de 0 à 254 dans chacun d'eux.



Lorsqu'on a fait du test sur DHCP de chaque VLAN, ils ont obtenu l'adresse IP automatiquement grâce au serveur DHCP.



Donc, le DHCP fonctionne bien.

Étape 3 – Ajout de la DMZ et du routeur du FAI

Objectif : Créer une zone DMZ isolée accessible depuis Internet via un pare-feu et filtrer les flux grâce à des ACL.

<u>Création de l'interface DMZ sur l'ASA: le but est d'</u> interdire toute communication directe entre le réseau interne et la DMZ

ASA(config)# interface vlan 3
ASA(config-if)# no forward interface vlan 1 (# interdit l'accès direct entre inside et dmz)
ASA(config-if)# nameif dmz
ASA(config-if)# security-level 50
ASA(config-if)# ip address 192.168.1.1 255.255.255.0
ASA(config-if)# no shutdown

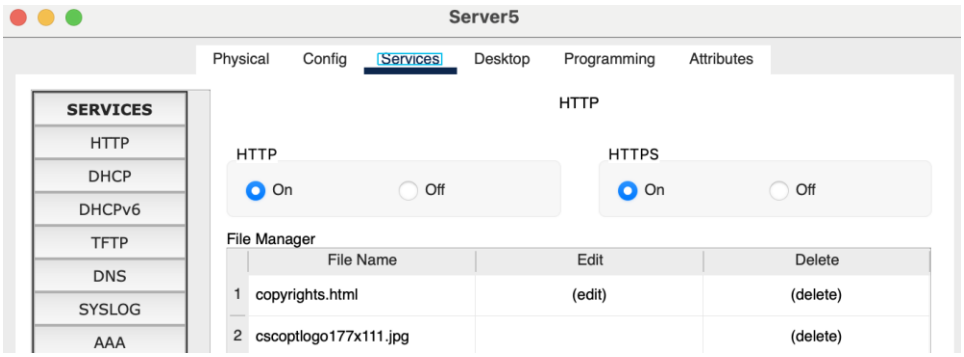
ASA(config)# interface ethernet0/2
ASA(config-if)# switchport access vlan 3

<u>Configuration de l'interface publique ASA :</u>

ASA(config)# interface vlan 2
ASA(config-if)# nameif outside
ASA(config-if)# security-level 0
ASA(config-if)# ip address 192.168.11.253 255.255.255.25Z
ASA(config-if)# no shutdown

ASA(config)# interface ethernet0/1
ASA(config-if)# switchport access vlan 2

Configuration du serveur Web dans la DMZ :



IP : 192.168.1.10

Passerelle : 192.168.1.1
Service HTTP et HTTPS activé

NAT dynamique (overload) : le but est d'avoir des routes statiques pour accéder à Internet et aux VLAN internes.

ASA(config)# route outside 0.0.0.0 0.0.0.0 192.168.11.254 1

ASA(config)# route inside 172.16.10.0 255.255.255.0 192.168.10.1 1

ASA(config)# route inside 172.16.20.0 255.255.255.0 192.168.10.1 1

ACL pour n'autoriser que les connexions HTTP/HTTPS vers la DMZ :

ASA(config)# access-list outside_access_in extended permit tcp any host 192.168.1.10 eq 443
ASA(config)# access-list outside_access_in extended permit tcp any host 192.168.1.2 eq www
ASA(config)# access-group outside_access_in in interface outside any any echo reply
ASA(config)# access-list outside_access_in extended permit tcp any host 192.168.1.10 eq domain
ASA(config)# access-list outside_access_in extended permit ip any any

ASA(config)# access-group outside_access_in in interface outside

Le pare-feu autorise seulement les réponses aux connexions lancées depuis l'intérieur et pour ce faire on a du filtre pour ce faire on a utilsé des class-map et des policy-maps:

ASA(config)# class-map inspection_default

ASA(config-cmap)# match default-inspection-traffic

ASA(config-cmap)# exit

ASA(config)# class-map inspection_inside_dmz

ASA(config-cmap)# match default-inspection-traffic

ASA(config-cmap)# exit

ASA(config)# class-map inspection_dmz_inside

ASA(config-cmap)# match default-inspection-traffic

ASA(config-cmap)# exit

ASA(config)# policy-map from-inside-to-dmz

ASA(config-pmap)# class inspection_inside_dmz

ASA(config-pmap-c)# inspect http

ASA(config-pmap-c)# inspect icmp

ASA(config-pmap-c)# exit

ASA(config-pmap)# exit

ASA(config)# policy-map from-dmz-to-inside

ASA(config-pmap)# class inspection_dmz_inside

ASA(config-pmap-c)# inspect http

ASA(config-pmap-c)# inspect icmp

ASA(config-pmap-c)# exit

ASA(config-pmap)# exit

Étape 4 – Ajout du réseau publique 8.8.0.0/16 et interconnexion avec le FAI

Objectif :
- Création du réseau 8.8.0.0/16 avec un client et un serveur DNS public.
- Configuration du routage EIGRP entre routeur Internet et FAI.
- Ajout de l'enregistrement DNS externe (www.entreprise.com → 1.1.1.253).
- Test d'un accès HTTP au serveur de la DMZ depuis le réseau public.

Configuration du routeur Le FAI sert de lien entre l'ASA et le routeur de test.com, avec du NAT overload pour permettre l'accès Internet et des NAT statiques pour les serveurs Web :

FAI(config)#interface GigabitEthernet0/0

FAI(config-if)#description Vers Internet

FAI(config-if)#ip address 192.168.11.254 255.255.255.252

FAI(config-if)#ip nat inside

FAI(config-if)#duplex auto

FAI(config-if)#speed auto

FAI(config-if)#exit

FAI(config)#interface GigabitEthernet0/1

FAI(config-if)#description Vers pare-feu ASA

FAI(config-if)#ip address 1.1.1.1 255.255.255.0

FAI(config-if)#ip access-group 100 out

FAI(config-if)#ip nat outside

FAI(config-if)#duplex auto

FAI(config-if)#speed auto

FAI(config-if)#exit

FAI(config)#interface Vlan1

FAI(config-if)#no ip address

FAI(config-if)#shutdown

FAI(config-if)#exit

Ici le but est de permettre à l'entreprise de joindre test.com et que test.com puissent joindre l'entreprise :

FAI(config)#router eigrp 10

FAI(config-router)#passive-interface GigabitEthernet0/0

FAI(config-router)#network 192.168.11.0 0.0.0.3

FAI(config-router)#network 1.1.1.0 0.0.0.255

FAI(config-router)#exit

FAI(config)#ip nat pool ent 1.1.1.2 1.1.1.2 netmask 255.255.255.0

FAI(config)#ip nat inside source list 1 pool ent overload

FAI(config)#ip nat inside source static 192.168.1.2 1.1.1.253

FAI(config)#ip nat inside source static 192.168.1.10 1.1.1.250

FAI(config)#ip classless

FAI(config)#ip route 172.16.10.0 255.255.255.0 192.168.11.253

FAI(config)#ip route 172.16.0.0 255.255.255.0 192.168.11.253

FAI(config)#ip route 172.16.20.0 255.255.255.0 192.168.11.253

FAI(config)#ip route 10.0.0.0 255.255.255.0 192.168.11.253

FAI(config)#ip route 192.168.1.0 255.255.255.0 192.168.11.253

FAI(config)#access-list 1 permit 172.16.0.0 0.15.255.255

FAI(config)#access-list 1 deny 192.168.0.0 0.0.255.255

FAI(config)#access-list 100 deny ip 172.16.0.0 0.15.255.255 any

FAI(config)#access-list 100 deny ip 10.0.0.0 0.255.255.255 any

FAI(config)#access-list 100 permit ip any any

FAI(config)#ip flow-export version 9

Pour le routeur entreprise j'ai tapé ces commandes :

Routeur(config)#interface GigabitEthernet0/0

Routeur(config-if)#ip address 1.1.1.254 255.255.255.0

Routeur(config-if)#duplex auto

Routeur(config-if)#speed auto

Routeur(config-if)#exit

Routeur(config)#interface GigabitEthernet0/1

Routeur(config-if)#ip address 1.1.2.129 255.255.255.252

Routeur(config-if)#duplex auto

Routeur(config-if)#speed auto

Routeur(config-if)#exit

Routeur(config)#router eigrp 10

Routeur(config-router)#redistribute static

Routeur(config-router)#passive-interface GigabitEthernet0/1

Routeur(config-router)#network 1.1.1.0 0.0.0.255

Routeur(config-router)#network 1.1.2.128 0.0.0.3

Routeur(config-router)#exit

Routeur(config)#ip classless

Routeur(config)#ip route 8.8.0.0 255.255.0.0 1.1.2.130

La on config le routeur test pour pouvoir tout relié :

Routeur(config)#interface GigabitEthernet0/0

Routeur(config-if)#ip address 1.1.2.130 255.255.255.252

Routeur(config-if)#exi

Routeur(config)#interface GigabitEthernet0/1

Routeur(config-if)#ip address 8.8.8.1 255.255.0.0

Routeur(config-if)#exit

Routeur(config)#ip route 1.1.1.0 255.255.255.0 1.1.2.129

Et pour finir pour que tout marche j'ai ajouté ces commande sur le switche qui relie les pc au routeur :

spanning-tree mode pvst
spanning-tree extend system-id

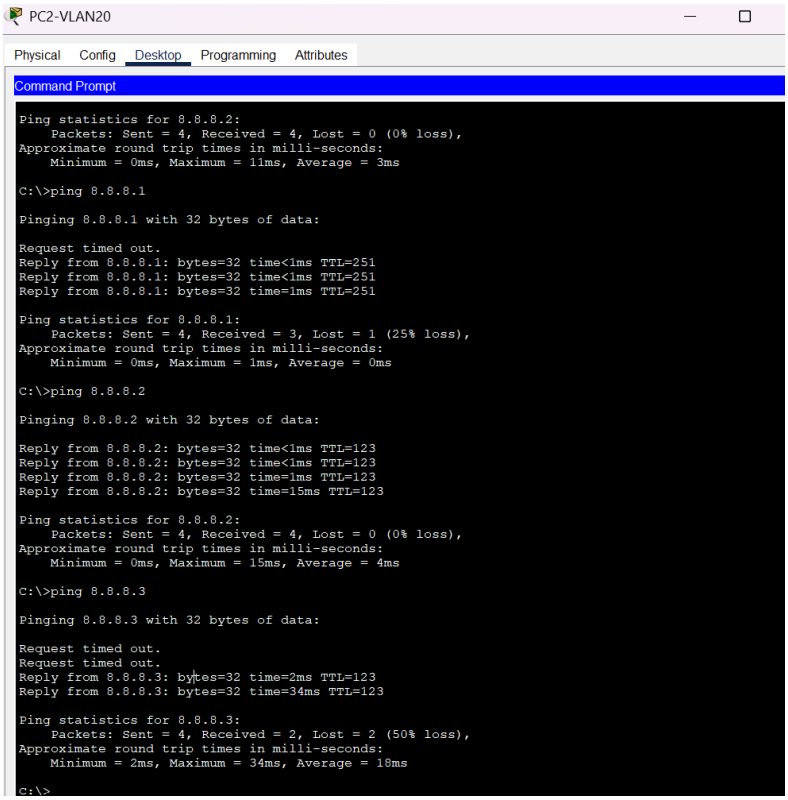
Verification :

Ping 8.8.8.1 correspond à l'ip du routeur test.com
Ping 8.8.8.2 correspond à l'ip du client 2 test.com
Ping 8.8.8.3 correspond à l'ip du client 3 test.com

Tests de validation :

- `ping www.test.com` depuis un client interne → OK
- `ping www.entreprise.com` depuis test.com → OK
- `telnet www.entreprise.com 80` → OK (HTTP)
- `telnet www.entreprise.com 443` → OK (HTTPS)
- `telnet www.entreprise.com 21` → Refusé (FTP bloqué par ACL)

Ces résultats confirment que l'accès est sécurisé, les DNS fonctionnent, et les flux sont correctement filtrés.

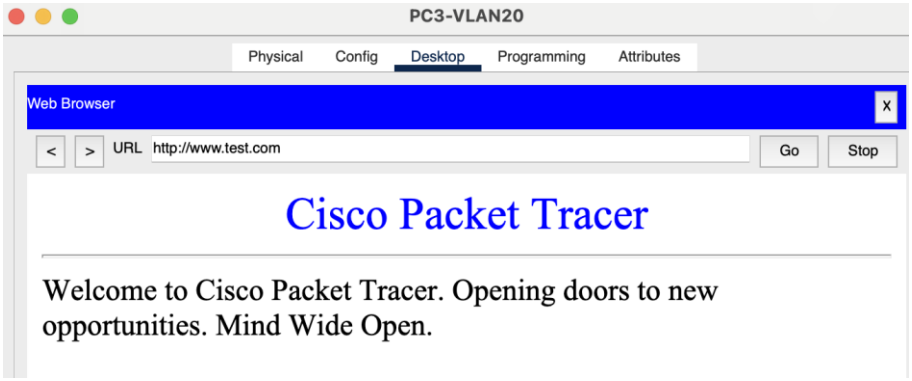


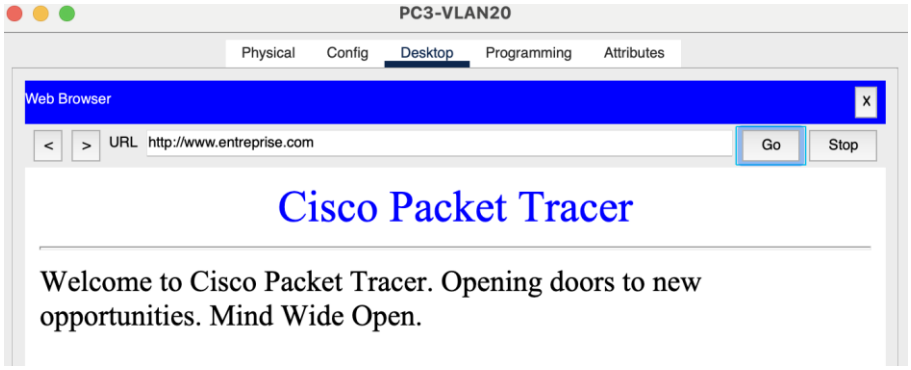
```
C:\>ping www.test.com

Pinging 8.8.8.2 with 32 bytes of data:

Reply from 8.8.8.2: bytes=32 time=2ms TTL=123
Reply from 8.8.8.2: bytes=32 time=7ms TTL=123
Reply from 8.8.8.2: bytes=32 time<1ms TTL=123
Reply from 8.8.8.2: bytes=32 time<1ms TTL=123

Ping statistics for 8.8.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\>ping www.entreprise.com

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 192.168.1.2: bytes=32 time=1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126
Reply from 192.168.1.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

On bloque l'acces vers l'interieur quand on est à l'extérieur vérifier grâce au ping :

```
C:\>ping 192.168.1.2

Pinging 192.168.1.2 with 32 bytes of data:

Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.

Ping statistics for 192.168.1.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 172.16.10.2

Pinging 172.16.10.2 with 32 bytes of data:

Reply from 8.8.8.1: Destination host unreachable.
Request timed out.
Reply from 8.8.8.1: Destination host unreachable.
Reply from 8.8.8.1: Destination host unreachable.

Ping statistics for 172.16.10.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

On peut accéder le site web de www.test.com et www.entreprise.com depuis les PCs intérieur :





Conclusion

Ce projet nous a permis de concevoir et de mettre en œuvre une architecture réseau complète pour une petite entreprise, en respectant des exigences à la fois fonctionnelles et sécuritaires. Grâce à la segmentation en VLANs, au routage inter-VLAN via un MLS, et à la mise en place d'un pare-feu ASA, nous avons structuré un réseau performant, cloisonné et sécurisé.

L'intégration des services DHCP et DNS a permis une gestion automatisée des configurations réseau, tandis que la DMZ a rendu possible l'exposition sécurisée d'un serveur web vers l'extérieur. L'utilisation du NAT dynamique et statique, combinée à des ACL rigoureuses, a garanti un accès contrôlé aux ressources tout en préservant l'intégrité du réseau interne.

Les différents tests de connectivité et de sécurité valident le bon fonctionnement de l'ensemble des services. En somme, ce projet nous a permis d'appliquer concrètement des notions théoriques en réseau, sécurité et administration système, tout en développant une vraie logique d'architecture.